

Huawei Qiankun

More Documents

Issue	01
Date	2024-01-25



Copyright © Huawei Technologies Co., Ltd. 2024. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Technologies Co., Ltd.

Trademarks and Permissions



HUAWEI and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Security Declaration

Vulnerability

Huawei's regulations on product vulnerability management are subject to the *Vul. Response Process*. For details about this process, visit the following web page:

<https://www.huawei.com/en/psirt/vul-response-process>

For vulnerability information, enterprise customers can visit the following web page:

<https://securitybulletin.huawei.com/enterprise/en/security-advisory>

Contents

1 Specifications.....	1
1.1 CloudCampus Service.....	2
1.2 Border Protection and Response.....	55
1.3 Huawei Qiankun App.....	58
2 Introduction to Licenses.....	62
2.1 Before You Start.....	62
2.2 License-related Concepts.....	62
2.3 License Control Items.....	63
3 Device Alarm Handling.....	64
3.1 V300 AR Alarms.....	64
3.1.1 ALM-4287406190 A Device Is Reset.....	64
3.1.2 ALM-4287373328 A Board Is Removed.....	65
3.1.3 ALM-4287373329 A Board Is Inserted.....	67
3.1.4 ALM-4287373322 Hardware fault.....	68
3.1.4.1 ALM-4287373322 Hardware fault 132103.....	68
3.1.4.2 ALM-4287373322 Hardware fault 132105.....	69
3.1.4.3 ALM-4287373322 Hardware fault 132106.....	71
3.1.4.4 ALM-4287373322 Hardware fault 132121.....	72
3.1.4.5 ALM-4287373322 Hardware fault 132128.....	74
3.1.4.6 ALM-4287373322 Hardware fault 132131.....	75
3.1.4.7 ALM-4287373322 Hardware fault 132137.....	77
3.1.4.8 ALM-4287373322 Hardware fault 132146.....	78
3.1.4.9 ALM-4287373322 Hardware fault 132154.....	80
3.1.5 ALM-4287373416 Insufficient Storage Space.....	81
3.1.6 ALM-4287373398 System Rollback.....	83
3.1.7 ALM-4287373404 CPU Utilization Exceeds the Threshold.....	85
3.1.8 ALM-4287373406 Memory Utilization Exceeds the Threshold.....	86
3.1.9 ALM-4287373399 Storage Media Remove.....	88
3.1.10 ALM-4287373400 Storage Media Is Inserted.....	89
3.1.11 ALM-4285734913 IPSec Tunnel Is Deleted.....	90
3.1.12 ALM-4286128130 The Status of Hub NHRP Is Up.....	93
3.1.13 ALM-4286128131 The Status of Hub NHRP Is Down.....	95

3.1.14 ALM-3488620545 The Status of the Link Is Down.....	96
3.1.15 ALM-4287373418 Battery fault.....	98
3.1.16 ALM-4287373420 Battery low.....	99
3.1.17 ALM-4287373386 The Temperature Is Not Within the Threshold.....	100
3.1.18 ALM-3491241985 The BGP Neighbor Is Changed.....	102
3.1.19 ALM-3491241990 The BGP Neighbor Is Disconnected.....	109
3.1.20 ALM-4288421943 VM CPU Usage Exceeding the Threshold.....	118
3.1.21 ALM-4288421944 VM Memory Usage Exceeding the Threshold.....	119
3.1.22 ALM-4288421945 VM State Exception.....	120
3.1.23 ALM-1880563716 The OSPF Neighbor Is Disconnected.....	122
3.1.24 ALM-4287766530 The CA certificate is nearly expired.....	125
3.1.25 ALM-4287766531 The local certificate is invalid.....	127
3.1.26 ALM-4287766532 The Local Certificate Is About to Expire.....	128
3.1.27 ALM-4287766533 The CRL Is Invalid.....	130
3.1.28 ALM-4287766534 The CRL Is About to Expire.....	131
3.1.29 ALM-157024261 The License Is About to Expire.....	132
3.1.30 ALM-1098063877 NQA ICMP Test Failed.....	133
3.1.31 ALM-3491242000 The number of BGP routes exceeded the maximum number that is allowed...	135
3.1.32 ALM-3491242001 The ratio of BGP routes to the maximum number that is allowed exceeded the alarm threshold.....	137
3.1.33 ALM-3276800300 The session resources were overloaded.....	139
3.1.34 ALM-3276800301 The evpn connection has entered the down state.....	140
3.1.35 ALM-3276800302 The number of evpn connections has reached the maximum number.....	142
3.1.36 ALM-3276800303 Power is unusable.....	143
3.1.37 ALM-3276800304 The number of connections has reached the threshold value.....	144
3.1.38 ALM-3276800306 The ms-channel has entered the down state.....	146
3.1.39 ALM-3276800320 Fan Is Invalid.....	147
3.1.40 ALM-3276800321 Fan Has Been Removed.....	148
3.1.41 ALM-3276800322 The Power Module Is Removed.....	150
3.1.42 ALM-303046420 RDB restore have failed Report.....	151
3.1.43 ALM-303046419 SPR Site Link Degrade.....	152
3.1.44 ALM-3235651584 MIB Information Change.....	153
3.1.45 ALM-3236306944 IPv6 Interface Status Change.....	154
3.1.46 ALM-3244957696 IP Address Change.....	157
3.1.47 ALM-4285734912 IPSec tunnel start.....	158
3.1.48 ALM-4285734925 IPSec Negotiation Fails.....	160
3.1.49 ALM-4286193664 The SPR link status has changed.....	166
3.1.50 ALM-4287373387 Temperature back to normal level.....	168
3.1.51 ALM-4287373001 The Device ACL Resources Were Insufficient.....	169
3.1.52 ALM-4287373002 The device acl resources were overloaded.....	170
3.1.53 ALM-303046881 The forwarding CPU usage exceeds the threshold.....	171
3.1.54 ALM-303046882 The forwarding memory usage exceeds the threshold.....	172
3.1.55 ALM-303046883 The forwarding single-core CPU usage exceeds the threshold.....	173

3.1.56 ALM-303046884 The device ESN has been changed.....	174
3.1.57 ALM-3224641536 The status of VRRP changed to master.....	175
3.1.58 ALM-3224641538 The state of VRRP changed from master to other state.....	178
3.1.59 ALM-3488620546 Interface Monitor Input Rate Rising.....	181
3.1.60 ALM-4285603840 NAT Packet Discard.....	183
3.1.61 ALM-3245219843 Ethernet ARP IP Conflict Event.....	184
3.1.62 ALM-3224903681 User Login.....	186
3.1.63 ALM-3224903682 User Login Fail.....	187
3.1.64 ALM-3224903683 User Logout.....	188
3.1.65 ALM-4286193665 The Current Link of the SPR Service Profile Changed.....	189
3.1.66 ALM-1880563712 The status of the OSPF interface was down.....	191
3.1.67 ALM-4289404934 All connections between sites have entered down state.....	194
3.1.68 ALM-4289601651 The number of forward sessions has reached the threshold value.....	197
3.1.69 ALM-4289601647 The backup link is in use.....	199
3.1.70 ALM-4289601648 RDB file recovery.....	200
3.1.71 ALM-4289601650 The number of connections has reached the threshold value.....	201
3.1.72 ALM-135471746 hwDeviceFaultAlarm.....	202
3.2 V500 Firewall Alarms.....	203
3.2.1 ALM-303046708 CPU usage exceeds the threshold.....	203
3.2.2 ALM-303046707 Memory usage exceeds the threshold.....	205
3.2.3 ALM-303046710 A card has stopped working.....	206
3.2.3.1 ALM-303046710 A card has stopped working 132626.....	206
3.2.3.2 ALM-303046710 A card has stopped working 132627.....	207
3.2.4 ALM-303046713 The power supply is invalid.....	208
3.2.5 ALM-303046700 The fan module is invalid.....	210
3.2.6 ALM-303046698 The card or subcard temperature is too high 143617.....	211
3.2.7 ALM-135462939 The fan module is removed.....	212
3.3 V200 LSW Alarms.....	213
3.3.1 ALM-135462942 The optical module is invalid.....	213
3.3.1.1 ALM-135462942 The optical module is invalid 136193.....	213
3.3.1.2 ALM-135462942 The optical module is invalid 136194.....	215
3.3.1.3 ALM-135462942 The optical module is invalid 136195.....	216
3.3.1.4 ALM-135462942 The optical module is invalid 136196.....	218
3.3.1.5 ALM-135462942 The optical module is invalid 136201.....	219
3.3.1.6 ALM-135462942 The optical module is invalid 136202.....	221
3.3.1.7 ALM-135462942 The optical module is invalid 136203.....	222
3.3.1.8 ALM-135462942 The optical module is invalid 136220.....	223
3.3.1.9 ALM-135462942 The optical module is invalid 136221.....	225
3.3.1.10 ALM-135462942 The optical module is invalid 136222.....	226
3.3.1.11 ALM-135462942 The optical module is invalid 136223.....	227
3.3.1.12 ALM-135462942 The optical module is invalid 136224.....	229
3.3.2 ALM-303046703 The power supply is removed 136448.....	230

3.3.3 ALM-303046702 The power module is installed 136448.....	231
3.3.4 ALM-303046701 Power supply is invalid.....	232
3.3.4.1 ALM-303046701 Power supply is invalid 136961.....	232
3.3.4.2 ALM-303046701 Power supply is invalid 136966.....	233
3.3.4.3 ALM-303046701 Power supply is invalid 136969.....	234
3.3.4.4 ALM-303046701 Power supply is invalid 136972.....	236
3.3.4.5 ALM-303046701 Power supply is invalid 136973.....	237
3.3.4.6 ALM-303046701 Power supply is invalid 136984.....	238
3.3.5 ALM-303046657 The fan module is removed 137216.....	239
3.3.6 ALM-303046656 The fan is faulty.....	240
3.3.6.1 ALM-303046656 The fan is faulty 139264.....	240
3.3.6.2 ALM-303046656 The fan is faulty 139266.....	241
3.3.7 ALM-303046661 The CPU usage of the device exceeds the alarm threshold.....	242
3.3.8 ALM-303046660 The memory usage of the device exceeds the alarm threshold.....	243
3.3.9 ALM-303046659 The temperature is abnormal.....	244
3.3.9.1 ALM-303046659 The temperature is abnormal 140544.....	245
3.3.9.2 ALM-303046659 The temperature is abnormal 140545.....	246
3.3.9.3 ALM-303046659 The temperature is abnormal 143624.....	248
3.3.10 ALM-303046658 The PD connected to the interface is powered off.....	250
3.3.11 ALM-303046665 PoE power supply is enabled on the port.....	252
3.3.12 ALM-134807555 The PD is connected.....	253
3.3.13 ALM-303046664 This PD is disconnected.....	253
3.3.14 ALM-303046663 The PD classes are invalid.....	254
3.3.15 ALM-303046662 The PD classes exceed the threshold.....	256
3.3.16 ALM-303046674 The Local Priority of the PD Is Different from the Priority Obtained Through LLDP	257
3.3.17 ALM-303046673 The Power Consumption of the PSE Exceeds the Upper Limit.....	258
3.3.18 ALM-303046672 The PoE power module is abnormal.....	259
3.3.19 ALM-303046425 The link is disconnected.....	260
3.3.20 ALM-3276800000 Indicates that SFP is not certified 136192.....	261
3.3.21 ALM-3276800001 Indicates that temperature exceeded the upper pre-alarm limit.....	263
3.3.22 ALM-3276800002 Indicates that temperature exceeded the lower pre-alarm limit.....	265
3.3.23 ALM-3276800003 Indicates that chip exception 67590.....	267
3.3.24 ALM-3276800004 A Fan Module Does Not Work Properly.....	268
3.3.25 ALM-3276800005 Indicates that PHY chip abnormal 67861.....	270
3.3.26 ALM-3276800006 Indicates that Optical module Tx power is too low.....	271
3.3.27 ALM-3276800007 Indicates that Optical module Rx power is too low.....	273
3.3.28 ALM-3276800008 Indicates that power loss 67967.....	275
3.3.29 ALM-3276800009 Indicates that power abnormal 67966.....	276
3.3.30 ALM-3276800010 Indicates that Tx Power Exceed Major.....	277
3.3.31 ALM-3276800011 Indicates that Rx Power Exceed Major.....	279
3.3.32 ALM-3276800012 Indicates that PHY abnormal 67958.....	280
3.3.33 ALM-3276800013 Indicates that LAN Switch abnormal 67962.....	282

3.3.34 ALM-3276800014 MP reached AC through the Ethernet port notify.....	283
3.3.35 ALM-3276800015 Indicates that CPLD Check abnormal 67963.....	284
3.3.36 ALM-3276800016 MPP joins AC through the air notify.....	285
3.3.37 ALM-3276800017 Indicates that FPGA Check abnormal 67964.....	286
3.3.38 ALM-3276800018 Indicates that USB abnormal 68072.....	287
3.3.39 ALM-3276800019 Indicates that USB 5v Power abnormal 68074.....	288
3.3.40 ALM-3276800020 Indicates that I2C abnormal 68080.....	289
3.3.41 ALM-3276800021 Indicates that RTC abnormal 68082.....	290
3.3.42 ALM-3276800022 Indicates that optical module power abnormal.....	292
3.3.42.1 ALM-3276800022 Indicates that optical module power abnormal 136193.....	294
3.3.42.2 ALM-3276800022 Indicates that optical module power abnormal 136194.....	295
3.3.42.3 ALM-3276800022 Indicates that optical module power abnormal 136195.....	297
3.3.42.4 ALM-3276800022 Indicates that optical module power abnormal 136196.....	298
3.3.43 ALM-3276800023 Network heartbeat.....	300
3.3.44 ALM-3276800024 PoE chip fault 68084.....	301
3.3.45 ALM-3276800025 Indicates that the service configurations exceed the recommended threshold.....	302
3.3.46 ALM-3276800026 Indicates that the service configurations failed.....	305
3.3.47 ALM-3276800028 Indicates that board fail.....	306
3.3.48 ALM-3276800029 Indicates that board invalid.....	315
3.3.49 ALM-3276800030 The number of VAP instances has exceeded the maximum.....	318
3.3.50 ALM-3276800031 Indicates that card fail.....	319
3.3.51 ALM-3276800032 Indicates that card invalid.....	320
3.3.52 ALM-3276800033 Optical Module Detection Failed.....	323
3.3.53 ALM-3276800034 The IGMP snooping bandwidth of VAP has reached the maximum.....	324
3.3.54 ALM-3276800035 The IGMP Snooping User of VAP Has Reached the Upper Threshold.....	325
3.3.55 ALM-3276800036 An AP Detects that the Soft-GRE Tunnel Is Down.....	327
3.3.56 ALM-3276800037 Communicate Error.....	328
3.3.57 ALM-3276800038 The Voltage of the Power Supply Is Higher than the Upper Threshold or Falls Below the Lower Threshold.....	330
3.3.58 ALM-3276800039 VAP create fail.....	334
3.3.59 ALM-3276800040 AP has the max number of stations notify.....	335
3.3.60 ALM-3276800041 RADIO reach the max number of stations notify.....	336
3.3.61 ALM-3276800042 Indicates that the optical power exceeds the upper warning threshold or falls below the lower warning threshold.....	337
3.3.61.1 ALM-3276800042 Indicates that the optical power exceeds the upper warning threshold or falls below the lower warning threshold 136220.....	337
3.3.61.2 ALM-3276800042 Indicates that the optical power exceeds the upper warning threshold or falls below the lower warning threshold 136221.....	339
3.3.61.3 ALM-3276800042 Indicates that the optical power exceeds the upper warning threshold or falls below the lower warning threshold 136222.....	340
3.3.61.4 ALM-3276800042 Indicates that the optical power exceeds the upper warning threshold or falls below the lower warning threshold 136223.....	342
3.3.62 ALM-3276800043 Indicates that the optical power exceeds the upper alarm threshold or falls below the lower alarm threshold.....	344

3.3.62.1 ALM-3276800043 Indicates that the optical power exceeds the upper alarm threshold or falls below the lower alarm threshold 136193.....	344
3.3.62.2 ALM-3276800043 Indicates that the optical power exceeds the upper alarm threshold or falls below the lower alarm threshold 136194.....	346
3.3.62.3 ALM-3276800043 Indicates that the optical power exceeds the upper alarm threshold or falls below the lower alarm threshold 136195.....	347
3.3.62.4 ALM-3276800043 Indicates that the optical power exceeds the upper alarm threshold or falls below the lower alarm threshold 136196.....	349
3.3.63 ALM-3276800044 An Optical Module Installed on the Device Is Not a Huawei-Certified Optical Module.....	351
3.3.64 ALM-3276800045 Indicates that the board ports conflict with each other.....	352
3.3.64.1 ALM-3276800045 Indicates that the board ports conflict with each other 147456.....	352
3.3.64.2 ALM-3276800045 Indicates that the board ports conflict with each other 147457.....	353
3.3.65 ALM-3276800046 Station author is error notify.....	354
3.3.66 ALM-3276800047 Patch deleted needs restart trap.....	356
3.3.67 ALM-3276800048 Input flow bandwidth usage exceeded the threshold.....	357
3.3.68 ALM-3276800049 VAP has the max number of stations notify.....	358
3.3.69 ALM-3276800050 Output flow bandwidth usage exceeded the threshold.....	359
3.3.70 ALM-3276800052 Packets are discarded for an error.....	360
3.3.71 ALM-3276800053 Hgig port state has changed.....	362
3.3.72 ALM-3276800054 Port state is always down.....	363
3.3.73 ALM-3276800055 Discards the runt packets.....	364
3.3.74 ALM-3276800056 The bridge loses the position of root bridge.....	365
3.3.75 ALM-3276800057 Station association is failed notify.....	367
3.3.76 ALM-3276800058 The port works in half duplex mode.....	369
3.3.77 ALM-3276800059 The port works in full duplex mode.....	370
3.3.78 ALM-3276800060 Physical entity port type changed.....	372
3.3.79 ALM-3276800061 ACL resource is full.....	373
3.3.80 ALM-3276800062 Tamper attack notify.....	374
3.3.81 ALM-3276800063 ACL resource lack.....	375
3.3.82 ALM-3276800064 The Layer 3 Resource Usage Reaches or Exceeds the Upper Threshold.....	377
3.3.83 ALM-3276800065 The STA Was Attacked by Replay Attacks.....	381
3.3.84 ALM-3276800066 Tamper attack notify.....	382
3.3.85 ALM-3276800067 The AP Security Level Was Lowered.....	384
3.3.86 ALM-3276800068 Address redirection attack notify.....	385
3.3.87 ALM-3276800069 SSID WEP Key IDs Conflict.....	387
3.3.88 ALM-3276800070 The Number of Users Associated with the AP Exceeds the Alarm Threshold....	388
3.3.89 ALM-3276800071 AP roam user number exceed threshold notify.....	389
3.3.90 ALM-3276800072 AP Access Channel Usage Exceeds the Threshold.....	391
3.3.91 ALM-3276800073 Radio signal environment deteriorates.....	392
3.3.92 ALM-3276800074 A Layer 3 service failed because of insufficient ACL resources.....	394
3.3.93 ALM-3276800075 Failed to execute the command.....	395
3.3.94 ALM-3276800076 IPv6 cannot be enabled on the interface because of insufficient system resources	397

3.3.95 ALM-3276800077 ND entries failed to be saved because of a hash conflict.....	398
3.3.96 ALM-3276800078 The switch detected an anomaly when periodically checking l3-forward-entries	399
3.3.97 ALM-3276800079 The card failed to deliver entries during VXLAN tunnel establishment due to a hash conflict.....	400
3.3.98 ALM-3276800080 The VXLAN-incapable card failed to decapsulate received VXLAN packets.....	401
3.3.99 ALM-3276800081 MAC address learning reached the limit.....	402
3.3.100 ALM-3276800082 MAC address information.....	404
3.3.101 ALM-3276800083 The MAC Address usage exceeds the threshold.....	406
3.3.102 ALM-3276800084 The MAC Address usage falls below the threshold.....	408
3.3.103 ALM-3276800085 The LPU is powered off.....	409
3.3.104 ALM-3276800086 The rapid-change of input broadcast exceeded the threshold.....	410
3.3.105 ALM-3276800087 The input rate change ratio exceeded the threshold.....	412
3.3.106 ALM-3276800088 The Output Rate Change Ratio Exceeded the Threshold.....	413
3.3.107 ALM-3276800089 IP Address-based Load Balancing on an Eth-Trunk Interface Fails to Take Effect for VXLAN Packets When It Functions as an Outbound Interface of VXLAN Packets.....	414
3.3.108 ALM-3276800090 Channel of radio is changed.....	416
3.3.109 ALM-3276800091 User attack occurred.....	418
3.3.110 ALM-3276800092 Port attack occurred.....	419
3.3.111 ALM-3276800094 StormCtrl occurred.....	421
3.3.112 ALM-3276800095 AP work mode is changed notify.....	423
3.3.113 ALM-3276800096 Gateway conflict.....	424
3.3.114 ALM-3276800097 Invalid ARP packet.....	426
3.3.115 ALM-3276800098 Dai drop alarm.....	427
3.3.116 ALM-3276800100 Global arp-miss exceed the speed-limit.....	428
3.3.117 ALM-3276800101 IPSG drop.....	430
3.3.118 ALM-3276800102 Global ICMP exceed the speed-limit.....	431
3.3.119 ALM-3276800103 Interface ICMP exceed the speed-limit.....	432
3.3.120 ALM-3276800104 The System Detected an Attack Source and Dropped Packets Sent from the Attack Source.....	433
3.3.121 ALM-3276800105 An Attack Source Is Detected and the Source Interface of Attack Packets to Error-Down State.....	435
3.3.122 ALM-3276800107 Auto-port-defend alarm.....	436
3.3.123 ALM-3276800108 User-packets-abnormal alarm.....	437
3.3.124 ALM-3276800109 Neighbor information is changed.....	438
3.3.125 ALM-3276800110 Global LLDP is enabled.....	440
3.3.126 ALM-3276800111 Global LLDP is disabled.....	441
3.3.127 ALM-3276800112 Local management address is changed.....	442
3.3.128 ALM-3276800113 The Rate of Received PDUs Exceeded the Threshold.....	443
3.3.129 ALM-3276800114 Co-Channel Interference Between APs Was Detected.....	444
3.3.130 ALM-3276800115 Adjacent Channel Interference Between APs Was Detected.....	446
3.3.131 ALM-3276800116 Jam of station is detected notify.....	448
3.3.132 ALM-3276800117 Interference from Other Devices Is Detected.....	449
3.3.133 ALM-3276800118 AP radio is down notify.....	450

3.3.134 ALM-3276800119 The Channel Usage by Roaming STAs Exceeds the Threshold.....	452
3.3.135 ALM-3276800120 Upload remote capture file notify.....	453
3.3.136 ALM-3276800121 The configuration of an AP is inconsistent with the actual attribute.....	454
3.3.137 ALM-3276800122 Detected rogue devices.....	456
3.3.138 ALM-3276800123 Detected attack devices.....	457
3.3.139 ALM-3276800124 Detected non-Wi-Fi devices.....	458
3.3.140 ALM-3276800125 AP not support configured channel.....	459
3.3.141 ALM-3276800126 The EIRP is unlawful due to high antenna gain.....	461
3.3.142 ALM-3276800127 Power of radio is changed.....	462
3.3.143 ALM-3276800130 Indicates that the stack-port state has changed to up.....	463
3.3.144 ALM-3276800131 Indicates that the stack-port state has changed to down.....	465
3.3.145 ALM-3276800132 Logical Ports of a Stack Were Connected Incorrectly.....	466
3.3.146 ALM-3276800133 Indicates a stack physical port link error.....	467
3.3.147 ALM-3276800134 Indicates that the stack physical port state has changed to down.....	469
3.3.148 ALM-3276800135 A Member Port that Has Been Added to a Logical Stack Port Becomes Up....	470
3.3.149 ALM-3276800136 Indicates that the other vlan conflicts with stack reserved-vlan.....	471
3.3.150 ALM-3276800137 Indicates that the stack set up failed.....	472
3.3.151 ALM-3276800138 Indicates that the device auto config stack port failed.....	473
3.3.152 ALM-3276800139 Indicates that the card types are different.....	476
3.3.153 ALM-3276800140 Failed to restore the system configurations.....	478
3.3.154 ALM-3276800141 The device was cold started.....	479
3.3.155 ALM-3276800142 The device was hot started, or the SNMP agent was enabled.....	479
3.3.156 ALM-3276800148 This object indicates the change of NTP synchronization status.....	480
3.3.157 ALM-3276800149 Detected rogue device.....	484
3.3.158 ALM-3276800150 AP changes to fault.....	485
3.3.159 ALM-3276800151 AP ping result.....	486
3.3.160 ALM-3276800152 AP is committed over.....	488
3.3.161 ALM-3276800153 The AP began to upgrade.....	489
3.3.162 ALM-3276800154 AP upgrade finished.....	490
3.3.163 ALM-3276800155 Unauthorized AP record exists.....	492
3.3.164 ALM-3276800156 The AP's Temperature Is Higher than the Upper Threshold.....	493
3.3.165 ALM-3276800157 The AP's temperature is too low.....	494
3.3.166 ALM-3276800158 AP CPU overload notify.....	496
3.3.167 ALM-3276800159 AP memory overload notify.....	497
3.3.168 ALM-3276800160 Dying gasp notify.....	499
3.3.169 ALM-3276800161 AC has system switched notify.....	500
3.3.170 ALM-3276800162 AP optical module received power is too high notify.....	502
3.3.171 ALM-3276800163 AP optical module temperature is too high notify.....	503
3.3.172 ALM-3276800164 AP optical module received power is too low notify.....	505
3.3.173 ALM-3276800165 AP optical module temperature is too low notify.....	507
3.3.174 ALM-3276800166 AP not support configured country code notify.....	508
3.3.175 ALM-3276800167 The AP cold boot.....	510

3.3.176 ALM-3276800168 AP hot boot.....	511
3.3.177 ALM-3276800169 AP CRC is abnormal notify.....	512
3.3.178 ALM-3276800170 The U-boot Version Does Not Match the AP Version.....	514
3.3.179 ALM-3276800171 Report ap name conflict.....	515
3.3.180 ALM-3276800172 AP License Notify.....	516
3.3.181 ALM-3276800173 AP IIC channel fault.....	517
3.3.182 ALM-3276800174 AP PHY CMOS fault.....	518
3.3.183 ALM-3276800175 AP FMEA fault.....	520
3.3.184 ALM-3276800176 AP optical insert.....	522
3.3.185 ALM-3276800177 AP optical remove.....	523
3.3.186 ALM-3276800178 AP receive invalid arp new trap.....	525
3.3.187 ALM-3276800179 AP software version is not match with AC software version.....	526
3.3.188 ALM-3276800180 AP optical module transfer power is too high notify.....	527
3.3.189 ALM-3276800181 AP optical module transfer power is too low notify.....	528
3.3.190 ALM-3276800182 All functions of the fan module failed.....	530
3.3.191 ALM-3276800183 A storage card is removed.....	531
3.3.192 ALM-3276800184 A storage card is inserted.....	532
3.3.193 ALM-3276800185 A port is powered off.....	533
3.3.194 ALM-3276800186 A port is powered on.....	535
3.3.195 ALM-3276800187 A port detects connection of a PD.....	537
3.3.196 ALM-3276800188 A port detects a PD whose current exceeds the threshold of the corresponding class.....	538
3.3.197 ALM-3276800189 The port priority is different from the PD priority.....	539
3.3.198 ALM-3276800190 The power load of a PoE card exceeds the upper limit.....	540
3.3.199 ALM-3276800191 Interface has turned into DOWN state.....	542
3.3.200 ALM-3276800192 The optical transceiver does not work normally.....	543
3.3.201 ALM-3276800193 Online AP number exceeded card specific.....	544
3.3.202 ALM-3276800194 The battery is low at the BLE site.....	545
3.3.203 ALM-3276800195 An exception occurs at the BLE site.....	546
3.3.204 ALM-3276800196 An IoT card is inserted.....	547
3.3.205 ALM-3276800197 The AP's internal BLE module fails.....	548
3.3.206 ALM-3276800198 Failed to start the server used by the IoT card.....	549
3.3.207 ALM-3276800199 SubFirmware is not match AP version.....	550
3.3.208 ALM-3276800201 An AP detected that a Bluetooth tag was detached.....	552
3.3.209 ALM-3276800202 The IoT Card Is Disconnected from the Server.....	553
3.3.210 ALM-3276800203 The IoT Card Does Not Match the Configured Type.....	554
3.3.211 ALM-3276800208 A iot card is removed.....	555
3.3.212 ALM-3276800209 A port detects disconnection of a PD.....	556
3.3.213 ALM-3276800210 The interface does not support the LRM optical module.....	558
3.3.214 ALM-3276800225 The current network cable quality is poor.....	559
3.3.215 ALM-3276800226 A Failure to detect the network cable quality.....	560
3.3.216 ALM-3276800227 AP power supply is insufficient.....	561
3.3.217 ALM-3276800228 An interface on an AP received a packet with an unauthorized MAC address.....	562

3.3.218 ALM-3276800229 The number of multicast and broadcast packets reported by an AP exceeded the alarm threshold.....	563
3.3.219 ALM-3276800230 The AP type configured on the AC did not match the actual AP type.....	564
3.3.220 ALM-3276800231 An AP detects that the Soft-GRE tunnel is Down.....	565
3.3.221 ALM-3276800232 The AP version is not recommended for the current AC.....	566
3.3.222 ALM-3276800234 The AP works in Limited mode due to insufficient power supply.....	567
3.3.223 ALM-3276800235 The WAPI certificate is nearly expired.....	569
3.3.224 ALM-3276800236 The WAPI certificate is invalid.....	570
3.3.225 ALM-4289601623 Virtual license is approaching expiration date alert.....	572
3.3.226 ALM-4289601624 Virtual license has expired.....	573
3.3.227 ALM-1099702272 Resource item is nearly used up.....	574
3.3.228 ALM-1099702273 License feature is near deadline.....	575
3.3.229 ALM-1099702274 Current license value is default.....	576
3.3.230 ALM-1099702275 Clear the alarm indicating that resources are nearly exhausted.....	577
3.3.231 ALM-1099702276 Clear the alarm indicating that the license feature is about to expire.....	578
3.3.232 ALM-1099702277 Clear the alarm indicating that the default license authorization value is used.....	579
3.3.233 ALM-1099702282 The mismatch between the device ESN and license file.....	580
3.3.234 ALM-1099702283 Clear the alarm indicating that the mismatch between the device ESN and license file.....	581
3.3.235 ALM-1099702284 Item is inactive.....	582
3.3.236 ALM-1099702285 Clear the alarm indicating that the item is inactive.....	583
3.3.237 ALM-3276800212 MAC address flapping occurs in a VSI.....	584
3.3.238 ALM-3276800213 MAC address flapping occurs in a BD.....	585
3.3.239 ALM-3276800214 A loop is detected on the Layer 2 network connected to the interface.....	587
3.3.240 ALM-3276800215 A loop is detected on the L2VPN network connected to the interface.....	588
3.3.241 ALM-3276800216 Port detected loopback.....	589
3.3.242 ALM-3276800217 A loop is detected in the network.....	591
3.3.243 ALM-3276800219 MAC address flapping has occurred.....	593
3.3.244 ALM-3276800305 Indicates that the CSS port state has changed to down.....	595
3.3.245 ALM-3276800474 The number of DHCPv6 Request messages that were discarded on an interface because they did not match the binding entries exceeded the threshold.....	596
3.3.246 ALM-3276800475 The number of the discarded DHCP packets in which the CHADDR field is inconsistent with the source MAC address exceeds the threshold on the interface.....	597
3.3.247 ALM-3276800476 The number of the discarded DHCP request packets that do not match the binding table exceeds the threshold on the interface.....	599
3.3.248 ALM-3276800477 The number of ND packets that were discarded on an interface because they did not match the binding entries exceeded the threshold.....	600
3.3.249 ALM-3276800478 The number of packets in a VLAN discarded by IPSG.....	601
3.3.250 ALM-3276800479 The number of the discarded DHCP reply packets on the untrusted interface exceeds the threshold.....	603
3.3.251 ALM-3276800480 The number of packets discarded by DAI exceeds the alarm threshold.....	604
3.3.252 ALM-3276800307 Interface input flow bandwidth usage exceeded the trap threshold.....	605
3.3.253 ALM-3276800308 Interface output flow bandwidth usage exceeded the trap threshold.....	607

3.3.254 ALM-4289601646 Indicates that the NETCONF database is abnormal.....	609
3.3.255 ALM-1707675687 The status of the terminal is abnormal.....	610
3.3.256 ALM-1707675688 Static MAC address flapping occurs.....	611
3.3.257 ALM-3276800485 The packet dropped by DAI exceeds the alarm threshold.....	613
3.3.258 ALM-3276800482 The Number of Flow Entry Resources Occupied by IFIT on a Device Exceeds the Threshold.....	614
3.3.259 ALM-3276800481 The Number of Flow Entry Resources Occupied by IFIT on a Card Exceeds the Threshold.....	615
3.3.260 ALM-3276800483 The DSCP Value of Packets Matching a Measurement Flow on a Card Conflicts with the IFIT Color Bit.....	616
3.3.261 ALM-3276800484 The error information of the command config.....	618
3.3.262 ALM-3276800238 The remote-unit firmware upgrade failed.....	618
3.3.263 ALM-4286849027 The number of incoming packets discarded due to congestion on an interface of a remote unit exceeds the threshold.....	620
3.3.264 ALM-4286849028 The number of outgoing packets discarded due to congestion on an interface of a remote unit exceeds the threshold.....	621
3.3.265 ALM-4286849029 The number of CRC error packets on an interface of a remote unit exceeds the threshold within a specified period of time.....	622
3.3.266 ALM-4286849030 The remote-unit is online.....	623
3.3.267 ALM-4286849031 The remote-unit is offline.....	624
3.3.268 ALM-4286849032 The authentication to the remote unit failed.....	625
3.3.269 ALM-4286849028 The remote-unit port is congested.....	626
3.3.270 ALM-3276800768 The CA certificate is nearly expired.....	627
3.3.271 ALM-3276800769 The local certificate is nearly expired.....	629
3.3.272 ALM-3276800770 The peer device cannot go online because Eth-Trunk auto-negotiation fails..	630
3.3.273 ALM-4289601668 The board has been removed.....	631
3.3.274 ALM-4289601669 The board has been inserted.....	632
3.4 WAC&AP Alarms.....	633
3.4.1 ALM-303046722 The Communication with the RADIUS Authentication Server Was Resumed.....	633
3.4.2 ALM-303046723 The Communication with the RADIUS Authentication Server Was Interrupted.....	634
3.4.3 ALM-303046724 The Communication with the RADIUS Accounting Server Was Resumed.....	636
3.4.4 ALM-303046725 The Communication with the RADIUS Accounting Server Was Interrupted.....	637
3.4.5 ALM-303046721 The Percentage of Successfully Authenticated NAC Users Reached the Lower Alarm Threshold.....	638
3.4.6 ALM-303046720 The Percentage of Successfully Authenticated NAC Users Reached the Upper Alarm Threshold.....	639
3.4.7 ALM-303046736 The Number of Used Addresses in the IP Address Pool Reached the Upper Alarm Threshold.....	640
3.4.8 ALM-303046737 The Number of Used Addresses in the IP Address Pool Reached the Lower Alarm Threshold.....	641
3.4.9 ALM-303046918 The ARP Packet Transmitting Rate Exceeded the Timestamp Suppression Rate Limit for ARP Packets.....	642
3.4.10 ALM-303046919 The Number of ARP Entries Exceeded the Upper Threshold.....	644
3.4.11 ALM-303046920 ARP Detects an IP Address Conflict.....	646
3.4.12 ALM-303046732 The Number of Global DHCP Users Reached the Upper Alarm Threshold.....	648

3.4.13 ALM-303046733 The Number of Global DHCP Users Reached the Lower Alarm Threshold.....	649
3.4.14 ALM-303046734 The Number of Global ND Users Reached the Upper Alarm Threshold.....	650
3.4.15 ALM-303046981 The Number of Global ND Users Reached the Lower Alarm Threshold.....	651
3.4.16 ALM-303046689 Device Temperature Reached the Threshold.....	652
3.4.17 ALM-303046913 A Storage Card Was Removed.....	654
3.4.18 ALM-303046917 Some Functions on the Card Were Invalid.....	655
3.4.19 ALM-303046916 A Card Experienced A Complete Failure.....	658
3.4.20 ALM-303046688 An Exception Occurred on the Card.....	660
3.4.21 ALM-303046682 An Optical Module Was Removed from the AP.....	662
3.4.22 ALM-303046683 An Optical Module Was Installed on the AP.....	663
3.4.23 ALM-303046960 The Optical Module Was Invalid.....	664
3.4.23.1 ALM-303046960 The Optical Module Was Invalid 136193.....	664
3.4.24 ALM-303046915 The Power Supply Was Removed.....	666
3.4.25 ALM-303046409 The Power Supply Experienced a Partial Failure.....	667
3.4.26 ALM-303046914 The Power Supply Was Invalid.....	668
3.4.27 ALM-303046690 CPU Usage Reached the Threshold.....	669
3.4.28 ALM-303046691 Memory Usage Reached the Threshold.....	671
3.4.29 ALM-303046964 Interface was deleted.....	673
3.4.30 ALM-303046961 Interface input flow bandwidth usage exceeded the trap threshold.....	674
3.4.31 ALM-303046962 Interface output flow bandwidth usage exceeded the trap threshold.....	675
3.4.32 ALM-13049866 The link is disconnected.....	676
3.4.33 ALM-303046410 An IP address has been changed.....	678
3.4.34 ALM-303046742 An IPSec tunnel is established.....	679
3.4.35 ALM-303046743 An IPSec tunnel is deleted.....	681
3.4.36 ALM-303046744 An IPSec policy is added.....	684
3.4.37 ALM-303046745 An IPSec policy is deleted.....	685
3.4.38 ALM-303046746 An IPSec policy is applied to an interface.....	686
3.4.39 ALM-303046747 The application of an IPSec policy is deleted from an interface.....	687
3.4.40 ALM-303046748 Reset IKE SA.....	688
3.4.41 ALM-303046749 Reset IPSec SA.....	689
3.4.42 ALM-303046750 The number of IPSec tunnels has reached 80% of the CPU or license limit threshold.....	690
3.4.43 ALM-303046751 The number of IPSec tunnels has reached 90% of the CPU or license limit threshold.....	691
3.4.44 ALM-303046752 The number of IKE peers dynamically created by the AC has reached 80% of the threshold.....	692
3.4.45 ALM-303046753 The number of IKE peers dynamically created by the firewall has reached 90% of the threshold.....	693
3.4.46 ALM-303046754 The IKE SA has been established.....	693
3.4.47 ALM-303046756 The number of IPSec tunnels has reached the limit supported by a single CPU or license.....	695
3.4.48 ALM-303046755 IPSec tunnel negotiation fails.....	695
3.4.49 ALM-303046977 An Interface Receives a Packet with an Insecure MAC Address.....	700
3.4.50 ALM-303046968 Receive illegal MAC.....	702

3.4.51 ALM-303046966 MAC address flapping occurs and the interface is blocked.....	703
3.4.52 ALM-303046965 Loop exist in vlan.....	705
3.4.53 ALM-303046967 MAC address learning reached the limit.....	706
3.4.54 ALM-303046929 A Port Enters the Discarding State.....	707
3.4.55 ALM-303046930 This Bridge Is No Longer the Root Bridge of the instance.....	709
3.4.56 ALM-303046932 The ROOT-Protection port received superior message.....	711
3.4.57 ALM-303046931 The edged-port that enabled BPDU-Protection will be shutdown, because it received BPDU packet.....	713
3.4.58 ALM-303046933 The LOOP-Protection port did not receive BPDU packets in prescriptive time.....	715
3.4.59 ALM-303046934 When the port receives a BPDU packet, the edged-port attribute will be disabled.....	716
3.4.60 ALM-303046935 The MSTP Process's Port has been set to discarding state because of detecting loopback.....	718
3.4.61 ALM-303046695 PoE power supply is shut down.....	719
3.4.62 ALM-303046694 PoE Power Usage Exceeds the Threshold.....	721
3.4.63 ALM-303046728 After server detection is enabled and the alarm action is configured, the device detects that the Portal server changes from Down to Up.....	722
3.4.64 ALM-303046729 After server detection is enabled and the alarm action is configured, the device detects that the Portal server changes from Up to Down.....	723
3.4.65 ALM-303046730 The number of online Portal users exceeded the upper alarm threshold.....	724
3.4.66 ALM-303046731 The number of online Portal users was equal to or smaller than the lower alarm threshold.....	726
3.4.67 ALM-303046921 The number of public IPv4 prefixes exceeded the maximum value.....	727
3.4.68 ALM-303046936 Attack occurred.....	728
3.4.69 ALM-303046937 Attack occurred.....	730
3.4.70 ALM-303046944 Gateway Conflict.....	731
3.4.71 ALM-303046945 ARP Entry Attack.....	732
3.4.72 ALM-303046946 Invalid Packet.....	734
3.4.73 ALM-303046947 The Number of Packets Discarded by DAI Reaches the Threshold.....	735
3.4.74 ALM-303046948 The Rate of ARP Packets Exceeds the Alarm Threshold.....	736
3.4.75 ALM-303046949 The Interface ARP Packet Speed Exceeds the Speed-limit Value.....	737
3.4.76 ALM-303046950 The Rate of ARP Miss Packets Exceeds the Alarm Threshold.....	738
3.4.77 ALM-303046951 The Rate of ICMP Packet Exceeds the Threshold.....	739
3.4.78 ALM-303046952 The Rate of ICMP Packets on an Interface Exceeds the Alarm Threshold.....	740
3.4.79 ALM-303046697 The AP Is Cold Restarted.....	741
3.4.80 ALM-303046696 The AP Is Hot Restarted.....	741
3.4.81 ALM-303046953 MD5 Authentication Failed.....	742
3.4.82 ALM-3416067 Abnormal Cable SNR.....	744
3.4.83 ALM-303046403 The Port Is Down, Resulting In A Failure to Detect the Network Cable Quality..	745
3.4.84 ALM-303046791 An AP Changes to Fault.....	746
3.4.85 ALM-303046792 AP Ping Result.....	747
3.4.86 ALM-303046793 AP Is Committed Over.....	749
3.4.87 ALM-303046795 Unauthorized AP Record Exists.....	750
3.4.88 ALM-303046798 AP CPU Overload Notify.....	751

3.4.89 ALM-303046799 The Memory Usage of an AP Exceeds the Upper Threshold.....	752
3.4.90 ALM-303046693 No STA Can Be Associated with the AP.....	754
3.4.91 ALM-303046801 AC Has System Switched Notify.....	755
3.4.92 ALM-303046800 Dying Gasp Notify.....	756
3.4.93 ALM-303046797 The AP's Temperature Is Too Low.....	758
3.4.94 ALM-303046796 The AP's Temperature Is Too High.....	759
3.4.95 ALM-303046803 AP Optical Module Received Power Is Too Low Notify.....	761
3.4.96 ALM-303046802 AP Optical Module Received Power Is Too High Notify.....	762
3.4.97 ALM-303046804 AP Optical Module Temperature Is Too High Notify.....	764
3.4.98 ALM-303046805 AP Optical Module Temperature Is Too Low Notify.....	766
3.4.99 ALM-303046806 The AP Does Not Support the Country Code Configured on the WAC.....	767
3.4.100 ALM-303046807 The AP Cold Boot.....	768
3.4.101 ALM-303046808 AP Hot Boot.....	770
3.4.102 ALM-303046809 AP CRC Is Abnormal Notify.....	771
3.4.103 ALM-303046811 Report AP Name Conflict.....	772
3.4.104 ALM-303046812 AP License Notify.....	773
3.4.105 ALM-303046813 AP IIC Channel Fault.....	774
3.4.106 ALM-303046814 AP PHY CMOS Fault.....	776
3.4.107 ALM-303046815 AP FMEA Fault.....	777
3.4.108 ALM-303046922 AP Optical Insert.....	779
3.4.109 ALM-303046923 AP Optical Remove.....	781
3.4.110 ALM-303046400 AP Receive Invalid ARP New Trap.....	782
3.4.111 ALM-303046924 AP Software Version Is Not Match with AC Software Version.....	783
3.4.112 ALM-303046782 Upload Remote Capture File Notify.....	784
3.4.113 ALM-303046757 MP Reached AC through the Ethernet Port Notify.....	785
3.4.114 ALM-303046758 MPP Joins AC through the Air Notify.....	786
3.4.115 ALM-303046927 AP Optical Module Transfer Power Is Too High Notify.....	787
3.4.116 ALM-303046938 AP Optical Module Transfer Power Is Too Low Notify.....	789
3.4.117 ALM-303046939 All Functions of the Fan Module Failed.....	791
3.4.118 ALM-303046940 A Storage Card Is Removed.....	792
3.4.119 ALM-303046401 A Storage Card Is Inserted.....	793
3.4.120 ALM-303046941 A Port Is Powered off.....	794
3.4.121 ALM-303046402 A Port Is Powered on.....	796
3.4.122 ALM-303046942 A Port Detects Connection of A PD.....	797
3.4.123 ALM-303046407 A Port Detects Disconnection of A PD.....	798
3.4.124 ALM-303046943 A Port Detects A PD Whose Current Exceeds the Threshold of the Corresponding Class.....	799
3.4.125 ALM-303046954 The Port Priority Is Different from the PD Priority.....	801
3.4.126 ALM-303046955 The Power Load of A PoE Card Exceeds the Upper Limit.....	802
3.4.127 ALM-303046956 Interface Has Turned into DOWN State.....	803
3.4.128 ALM-303046957 The Optical Transceiver Does Not Work Normally.....	805
3.4.129 ALM-303046765 VAP Has the Max Number of Stations Notify.....	806
3.4.130 ALM-4287373447 the Number of Users Connected to the AP Exceeds the Alarm Threshold.....	808

3.4.131 ALM-3416068 Low Power of A BLE Device.....	809
3.4.132 ALM-3416069 A BLE Device Goes Offline.....	810
3.4.133 ALM-3416070 Built-in Bluetooth Module Fault.....	811
3.4.134 ALM-303046972 An IoT Card Is Inserted.....	812
3.4.135 ALM-303046406 An IoT Card Is Removed.....	813
3.4.136 ALM-303046973 Failed to Start the Server Used By the IoT Card.....	814
3.4.137 ALM-303046974 SubFirmware Is Not Match AP Version.....	815
3.4.138 ALM-303046783 the AP Configuration Is Inconsistent with the Actual Attribute.....	816
3.4.139 ALM-303046987 the BLE Site Detached.....	817
3.4.140 ALM-303046991 AP Power Supply Is Insufficient.....	818
3.4.141 ALM-303046982 Interface Receive Insecure Mac-address.....	820
3.4.142 ALM-303046983 the Number of Multicast and Broadcast Packets Received on the AP Exceeds the Threshold 1000 pps for 10 Seconds.....	821
3.4.143 ALM-303046984 the Configured and Reported AP Types Are Different.....	822
3.4.144 ALM-303046985 An AP Detects that the Soft-GRE Tunnel Is Down.....	823
3.4.145 ALM-303046992 the AP Version Is Not Recommended for the Current AC.....	824
3.4.146 ALM-303046404 the Disk Usage of An AP Exceeds the Upper Threshold.....	825
3.4.147 ALM-303046405 the AP Works in Limited Mode Due to Insufficient Power Supply.....	826
3.4.148 ALM-303046738 the AP Works in Limited Mode Due to Insufficient Power Supply.....	828
3.4.149 ALM-303046794 AP Begins to Update.....	829
3.4.150 ALM-303046408 AP Upgrade Finished.....	830
3.4.151 ALM-303046810 The U-boot Version Does Not Match the AP Version.....	832
3.4.152 ALM-303046790 Detected Rogue Device.....	833
3.4.153 ALM-303046784 Detected Rogue Devices.....	835
3.4.154 ALM-303046785 Detected Attack Devices.....	836
3.4.155 ALM-303046786 Detected non-Wi-Fi Devices.....	838
3.4.156 ALM-303046773 Channel of Radio Is Changed.....	839
3.4.157 ALM-303046772 Radio Signal Environment Deteriorates.....	841
3.4.158 ALM-303046774 AP work mode is changed notify.....	843
3.4.159 ALM-303046775 Co-Channel Interference Between APs Was Detected.....	845
3.4.160 ALM-303046776 Adjacent Channel Interference Between APs Was Detected.....	846
3.4.161 ALM-303046777 Jam of station is detected notify.....	848
3.4.162 ALM-303046778 Interference from Other Devices Is Detected.....	849
3.4.163 ALM-303046779 AP radio is down notify.....	851
3.4.164 ALM-303046787 AP not support configured channel.....	852
3.4.165 ALM-303046788 The EIRP is unlawful due to high antenna gain.....	854
3.4.166 ALM-303046789 Power of radio is changed.....	855
3.4.167 ALM-4287373449 The number of users associated with the AP exceeds the alarm threshold.....	856
3.4.168 ALM-303046770 AP access user number exceed threshold notify.....	858
3.4.169 ALM-4287373448 The number of roaming users connected to the AP exceeds the alarm threshold.....	859
3.4.170 ALM-303046771 AP roam user number exceed threshold notify.....	860
3.4.171 ALM-303046704 AP Access Channel Utilization Exceeds the Threshold.....	861

3.4.172 ALM-303046781 The Channel Usage by Roaming STAs Exceeds the Alarm Threshold.....	862
3.4.173 ALM-303046766 RADIO reach the max number of stations notify.....	864
3.4.174 ALM-303046759 The number of VAP instances has exceeded the maximum.....	865
3.4.175 ALM-303046760 The IGMP snooping bandwidth of VAP has reached the maximum.....	866
3.4.176 ALM-303046761 The IGMP Snooping User of VAP Has Reached the Threshold.....	868
3.4.177 ALM-303046763 A VAP Fails to Be Created.....	869
3.4.178 ALM-303046767 Station author is error notify.....	872
3.4.179 ALM-303046768 Station association is failed notify.....	874
3.4.180 ALM-303046969 A User with an Invalid Certificate Accessed the Network.....	876
3.4.181 ALM-303046976 An STA Was Attacked by Replay Attacks.....	877
3.4.182 ALM-303046739 Tamper attack notify.....	879
3.4.183 ALM-303046740 The AP Security Level Was Lowered by Attacks.....	880
3.4.184 ALM-303046741 Address redirection attack notify.....	882
3.4.185 ALM-303046769 SSID WEP key conflict notify.....	883
3.4.186 ALM-303046988 The Local WAC Configuration Is Inconsistent with that on the Remote WAC...	885
3.4.187 ALM-3416071 AP Power Supply Insufficient.....	886
3.4.188 ALM-303046912 Disk usage exceeds the threshold.....	887
3.4.189 ALM-303046764 AP has the max number of stations notify.....	888
3.4.190 ALM-3416072 AP broadcast and multicast packets over threshold.....	889
3.4.191 ALM-3276800205 The IoT Card Is Disconnected from the Server.....	890
3.4.192 ALM-3276800206 The IoT card does not match the configured type.....	892
3.4.193 ALM-303046411 The WAPI certificate is nearly expired.....	893
3.4.194 ALM-303046412 The WAPI certificate is invalid.....	895
3.4.195 ALM-303046413 The CA certificate is invalid.....	896
3.4.196 ALM-303046414 The CA Certificate Is About to Expire.....	897
3.4.197 ALM-303046415 The local certificate is invalid.....	899
3.4.198 ALM-303046416 The local certificate is nearly expired.....	900
3.4.199 ALM-3276800218 System Rollback.....	901
3.4.200 ALM-303046417 Session resources exceed the threshold.....	902
3.4.201 ALM-1707675682 Container CPU utilization is greater than the alarm threshold.....	903
3.4.202 ALM-1707675683 Container memory usage above threshold.....	905
3.4.203 ALM-1707675684 Container storage space utilization too high alarm.....	906
3.4.204 ALM-1707675685 Abnormal operation of container.....	907
3.4.205 ALM-1707675686 Abnormal operation alarm of APP in container.....	909
3.4.206 ALM-303046418 NETCONF Database Exception.....	910
3.4.207 ALM-303046421 The EMDI session on the AP exceeds the threshold.....	911
3.4.208 ALM-303046422 The SIPFPM flow table on the AP exceeds the threshold.....	912
3.4.209 ALM-303046423 The number of SIPFPM flow tables on the AP reaches the maximum.....	913
3.4.210 ALM-303046424 The SIPFPM flow table on the AC reaches the upper limit.....	915
3.4.211 ALM-3276800750 The CA certificate is nearly expired.....	916
3.4.212 ALM-3276801006 The local certificate is nearly expired.....	917
3.4.213 ALM-4286849026 The CPE device generate an alarm.....	918

3.5 V600 Device Alarms.....	919
3.5.1 Common Alarms.....	919
3.5.1.1 ALM-15795031 CPU_BUSY.....	919
3.5.1.2 ALM-135462939 hwPowerInvalid.....	921
3.5.1.3 ALM-15795032 hwStorageUtilizationRisingAlarm.....	928
3.5.1.4 ALM-135462943 hwPowerRemove.....	930
3.5.1.5 ALM-135462937 hwFanRemove.....	932
3.5.1.6 ALM-135462925 hwBrdTempAlarm.....	933
3.5.1.7 ALM-139591683 linkDown.....	935
3.5.1.8 ALM-135462958 hwBoardInvalid.....	948
3.5.1.9 ALM-135462935 hwFanInvalid.....	958
3.5.1.10 ALM-135462966 hwFanFail.....	959
3.5.1.11 ALM-15795007 hwPKILocalCertInvalid.....	960
3.5.1.12 ALM-135463086 hwIfMonitorInputRateRising.....	961
3.5.1.13 ALM-135463087 hwIfMonitorOutputRateRising.....	963
3.5.1.14 ALM-135471444 hwOpticalUnauthorized.....	964
3.5.1.15 ALM-135463001 hwOpticalInvalid.....	965
3.5.1.16 ALM-135463100 hwIfMonitorCrcErrorRising.....	973
3.5.1.17 ALM-15795006 hwPKILocalCertNearlyExpired.....	975
3.5.1.18 ALM-135462976 hwBoardRemove.....	976
3.5.1.19 ALM-183312389 hwRadiusAuthServerDown.....	977
3.5.1.20 ALM-183312391 hwRadiusAcctServerDown.....	978
3.5.1.21 ALM-135462996 hwBoardFail.....	979
3.5.1.22 ALM-15795011 hwPKICACertInvalid.....	990
3.5.1.23 ALM-15795010 hwPKICACertNearlyExpired.....	991
3.5.1.24 ALM-15795009 hwPKICrInvalid.....	992
3.5.1.25 ALM-15795008 hwPKICrNearlyExpired.....	993
3.5.1.26 ALM-15795049 hwHrpDeviceID.....	994
3.5.1.27 ALM-135462941 hwPowerFail.....	996
3.5.1.28 ALM-135462923 hwBrdTempFatalAlarm.....	1000
3.5.1.29 ALM-157024261 hwGtlNearDeadline.....	1002
3.5.1.30 ALM-157024262 hwGtlDefaultValue.....	1003
3.5.1.31 ALM-135463092 hwChassisFail.....	1005
3.5.2 AR Alarms.....	1006
3.5.2.1 ALM-142147599 bgpBackwardTransition.....	1006
3.5.2.2 ALM-15794956 hwBgpPeerAddrFamilyRouteThresholdExceed.....	1014
3.5.2.3 ALM-15795089 hwBgpPeerAddrFamilyRouteExceed.....	1015
3.5.2.4 ALM-15795185 hwConnectionDownReport.....	1016
3.5.2.5 ALM-15795206 hwConnectionThresholdExceed.....	1018
3.5.2.6 ALM-15795205 hwConnectionMaxExceed.....	1020
3.5.2.7 ALM-15795258 hwSPRInstanceReport.....	1021
3.5.2.8 ALM-15795318 hwSessExceed.....	1024

3.5.2.9 ALM-15795117 hwSystemRollback.....	1025
3.5.2.10 ALM-15794965 hwSrPolicyDown.....	1026
3.5.2.11 ALM-15794966 hwSrPolicyResourceThresholdExceed.....	1027
3.5.2.12 ALM-15794967 hwSrPolicyResourceTotalCountExceed.....	1029
3.5.2.13 ALM-15795368 hwSiteDisconnect.....	1030
3.5.2.14 ALM-15795445 hwConnectionPolicyApplyFail.....	1033
3.5.2.15 ALM-215031809 hwSystemRollback.....	1034
3.5.2.16 ALM-15795156 HostUnitLinkAbnormal.....	1035
3.5.2.17 ALM-15795527 VMResourceInconsist.....	1036
3.5.3 LSW Alarms.....	1038
3.5.3.1 ALM-135462929 hwCommunicateError.....	1038
3.5.3.2 ALM-135462997 hwEntityInvalid.....	1039
3.5.3.3 ALM-135462998 hwCardFail.....	1043
3.5.3.4 ALM-135462999 hwCardInvalid.....	1044
3.5.3.5 ALM-134292070 hwPoePowerOff.....	1045
3.5.3.6 ALM-134292071 hwPoePdConnected.....	1047
3.5.3.7 ALM-134292072 hwPoePdDisconnected.....	1048
3.5.3.8 ALM-15795217 hwPoePdClassInvalid.....	1049
3.5.3.9 ALM-15795218 hwPoePdPriorityDifferent.....	1050
3.5.3.10 ALM-15795219 hwPoePowerOverUtilizationThreshold.....	1051
3.5.3.11 ALM-15795325 hwPoePowerOn.....	1052
3.5.3.12 ALM-15795346 hwPoePdClassOvercurrent.....	1053
3.5.3.13 ALM-223617026 hwMstpProRootLost.....	1054
3.5.3.14 ALM-15794194 hwGtlResourceUsedUp.....	1056
3.5.3.15 ALM-157163598 hwMflpBdAlarm.....	1057
3.5.3.16 ALM-161611792 hwStackLogicStackPortLinkErr.....	1058
3.5.3.17 ALM-157024263 hwGtlItemMismatch.....	1060
3.5.3.18 ALM-157155346 hwMflpVlanLoopAlarm.....	1060
3.5.3.19 ALM-157163596 hwBdMacLimitOverThresholdAlarm.....	1062
3.5.3.20 ALM-157163635 hwVxlanTunnelMacLimitOverThresholdAlarm.....	1063
3.5.3.21 ALM-257564679 hwVlanMacLimitOverThreshold.....	1064
3.5.3.22 ALM-257564680 hwPortMacLimitOverThreshold.....	1065
3.5.3.23 ALM-157163553 hwMacUsageRaisingInfo.....	1066
3.5.3.24 ALM-234102790 hwMacMovedQuietMaxUserAlarm.....	1067
3.5.3.25 ALM-234102791 hwMacMovedQuietUserClearAlarm.....	1068
3.5.3.26 ALM-233578498 hwMacQuietMaxUserAlarm.....	1069
3.5.3.27 ALM-233578499 hwMacQuietUserClearAlarm.....	1070
3.5.3.28 ALM-233574400 hwNACMaxUserAlarm.....	1071
3.5.3.29 ALM-234102786 hwMaxUclGroupIpNumAlarm.....	1072
3.5.3.30 ALM-233447431 hwMacAuthenMaxUserAlarm.....	1073
3.5.3.31 ALM-233443329 hwQuietUserClearAlarm.....	1074
3.5.3.32 ALM-233443328 hwQuietUserMaxAlarm.....	1075

3.5.3.33 ALM-233447430 hwSrvcfgEapMaxUserAlarm.....	1076
3.5.3.34 ALM-233574401 hwNACUserClearAlarm.....	1077
3.5.3.35 ALM-15795094 SRV6_LOCAL_SID_ROUTE_CONFLICT.....	1078
3.5.3.36 ALM-67706900 hwRuAuthFail.....	1079
3.5.3.37 ALM-67699723 hwRuMngFirmwareUpdateFail.....	1080
3.5.3.38 ALM-67699726 hwRuMngOffline.....	1081
3.5.3.39 ALM-67699725 hwRuMngOnline.....	1083
3.5.3.40 ALM-67706884 hwRuPortCrcErrorRising.....	1084
3.5.4 Firewall Alarms.....	1085
3.5.4.1 ALM-15795462 hwGtlDataDamaged.....	1085
3.5.4.2 ALM-15795028 hwIPSecNegotFail.....	1086
3.5.5 S380 Device Alarms.....	1090
3.5.5.1 ALM-135463092 hwChassisFail.....	1090
3.5.5.2 ALM-134292070 hwPoePowerOff.....	1092
3.5.5.3 ALM-15795219 hwPoePowerOverUtilizationThreshold.....	1093
3.5.5.4 ALM-135463086 hwIfMonitorInputRateRising.....	1095
3.5.5.5 ALM-135463087 hwIfMonitorOutputRateRising.....	1096
3.5.5.6 ALM-230432775 hwUsedIPReachThreshold.....	1097
3.5.5.7 ALM-157163553 hwMacUsageRaisingInfo.....	1098
3.5.5.8 ALM-157155346 hwMflpVlanLoopAlarm.....	1099
3.5.5.9 ALM-15795035 hwSecStatSessOverThreshold.....	1100
3.5.5.10 ALM-15795035 hwPacketDiscard.....	1101
3.5.5.11 ALM-139591683 linkDown.....	1101
3.5.5.12 ALM-135463100 hwIfMonitorCrcErrorRising.....	1114
3.5.5.13 ALM-15795032 hwStorageUtilizationRisingAlarm.....	1116
3.5.5.14 ALM-135462996 hwBoardFail.....	1118
3.5.5.15 ALM-135462925 hwBrdTempAlarm.....	1129
3.5.5.16 ALM-135463001 hwOpticalInvalid.....	1131
3.5.5.17 ALM-135462923 hwBrdTempFatalAlarm.....	1139
3.5.5.18 ALM-15794223 hwEthHalfDuplex.....	1141
3.5.5.19 ALM-135602186 RESTORE_CONFIGURATION_FAIL.....	1142

1 Specifications

- 1.1 CloudCampus Service
- 1.2 Border Protection and Response
- 1.3 Huawei Qiankun App

1.1 CloudCampus Service

Table 1-1 Huawei Qiankun CloudCampus Service specifications

Level-1 Category	Level-2 Category	Level-3 Category	Level-4 Category	Item	Description
Cloud-based network management	Resource management	Resource management	Device management	Cloud managed device management	Cloud managed devices refer to the devices that connect to the console through NETCONF Callhome. ARs, cloud APs, switches, and firewalls can be managed in this method. • Users can import device SNs, set device names and descriptions, and add devices to sites. • Users can delete devices one by one or in batches. • The console can display information about existing devices of a specific tenant. The displayed device information includes the device name, SN, status, site, model, license status, software version, and registration time. Devices can be filtered by status, site type, or keyword. • Device information, such as the device name, description, SN, and role, can be modified.
			File management (*)	File management (*)	• Allows users to upload various types of local files through the web UI, including software packages, patches, certificate files, and license files. • Allows users to view the file upload task list and stop or cancel an upload task. • Allows users to upload signature files of software packages or patches for verification. (Software packages and patches are managed using uUpgrade.)

Level-1 Category	Level-2 Category	Level-3 Category	Level-4 Category	Item	Description
	Network service configurations	NE registration	Protocol channel	Management mode (cloud managed devices)	Cloud managed devices proactively use the Call Home service to connect to the console through SSH channels.
			SN whitelist	-	An SN whitelist can be configured. Devices that are not whitelisted cannot be registered and managed, which improves security.
			NE authentication	-	Performs two-way authentication based on certificates and device SNs.
			Deployment modes	DHCP-based deployment	The DHCP Option 148 mode is used for on-premises deployment. After obtaining IP addresses, devices automatically connect to the Huawei Qiankun Cloud Platform.
				Registration query center-based deployment	After tenants import device SNs on the Huawei Qiankun Cloud Platform, the devices automatically connect to the registration query center for registration and onboarding. Currently, ARs do not support this deployment mode.
				CLI-based deployment	Users can connect to devices through the console port and run commands to specify the IP address of the Huawei Qiankun Cloud Platform to which the devices need to connect to onboard the devices.
				Others	- Barcode scanning-based deployment is supported. - Firewalls and ARs support USB-based deployment. - Only ARs support email-based deployment.

Level-1 Category	Level-2 Category	Level-3 Category	Level-4 Category	Item	Description
		Template management	Site configuration template management (*)	Site configuration template (*)	• Site templates can be created, viewed, modified, and deleted. • Site templates can be bound to and unbound from sites. • A site template can contain the following configurations: – Site-level configuration: BootROM, SNMP, local users, and NTP – AP parameters: radio, SSID, attack defense, wireless security, and DHCP – Firewall parameters: subnet, DNS, authentication, SSID, and traffic policy
				CLI-based site configuration template (*)	APs, ARs, firewalls, and switches support CLI-based site configuration templates.
				Site configuration template clone (*)	Site configuration templates can be cloned.

Level-1 Category	Level-2 Category	Level-3 Category	Level-4 Category	Item	Description
			Feature template (*)	Template-based switch port feature configuration (*)	• Port security: configures DHCP snooping, ND snooping, IPSG, DAI, port isolation, and storm control. One template can be bound to multiple switch ports. • Port VLAN: configures VLANs for access, trunk, and hybrid ports, default VLANs for ports, allowed VLANs, and voice VLANs. One template can be bound to multiple ports. • Port physical attribute: configures auto-negotiation and PoE. • Port ring network: configures STP and loop detection. One template can be bound to multiple ports. • Port traffic policy: configures a traffic policy specific to a port or port group. A traffic policy defines a DSCP value in the range from 0 (lowest) to 63 (highest) or an 802.1p priority in the range from 0 (lowest) to 7 (highest). • Interface-based application identification and application traffic statistics collection are supported.

Level-1 Category	Level-2 Category	Level-3 Category	Level-4 Category	Item	Description
				Template-based switch feature configuration (*)	• Device groups can be defined. • Traffic policies can be delivered to devices or device groups (only applicable to switches). A traffic policy can contain the following configurations: – Outbound, inbound, and bidirectional – Traffic classifier: 5-tuple and VLAN range – Traffic behavior: deny and permit – Traffic rate limiting: CIR, PIR, CBS, and PBS – Traffic priority: local priority, DSCP priority, and 802.1p priority
			Template management	Template management (*)	Allows users to create, modify, and delete service templates.

Level-1 Category	Level-2 Category	Level-3 Category	Level-4 Category	Item	Description
				Service template (*)	• ACL, dynamic ACL, URL, and URL category templates are supported. • RADIUS server, RADIUS relay server, HWTACACS server, and third-party Portal server templates are supported. • Authentication and bypass policy templates are supported. • Traffic classifier and traffic behavior templates are supported. • HQoS-related templates, including user-defined application templates and application scheduling templates, are supported. • IGMP snooping templates are supported. • WAN link templates are supported. • SNMP templates are supported to scan and discover traditional devices. • Firewall security zone templates and IP/MAC address sets can be managed. • SA applications can be customized.
			Device template information	Switch interface template (*)	Switch template management is supported, including adding, deleting, modifying, and viewing switch device templates. Switch interface features can be configured in switch device templates.
				CLI-based template (*)	CLI-based device configuration templates can be configured for APs, ARs, firewalls, and switches.

Level-1 Category	Level-2 Category	Level-3 Category	Level-4 Category	Item	Description
		Basic configuration management	Device name configuration	-	The console can deliver device names to devices to accurately identify the devices.
			Device administrator account password configuration	-	The console supports change of the password, service level, and supported service type of the device administrator account admin .
			Time configuration	-	- Time zones can be configured to enable devices to display the local time. - The Network Time Protocol (NTP) can be configured so that devices can synchronize time using NTP to ensure time accuracy.

Level-1 Category	Level-2 Category	Level-3 Category	Level-4 Category	Item	Description
		Layer 2 and Layer 3 network service management	Interface management	Interface configuration	- Ethernet interface information is displayed in a list. - The following interface configurations are supported: administrative status, description, auto-negotiation (rate and duplex mode), management VLAN auto-negotiation, VLAN ID, allowed VLANs, and voice VLAN. - Link neighbor discovery protocols LLDP and CDP can be configured. - The following port security configurations are supported: DHCP snooping, ND snooping, ARP snooping, DNS snooping, mDNS snooping, DAI, IPSG, storm suppression, and loop detection. - IP subnet-based VLAN assignment can be configured. - The function of generating SNMP traps upon status changes can be configured. - Dynamic MAC address collection can be configured. - Trust options, port isolation, storm control, loop detection, and PoE can be configured. - STP and edge ports can be configured.
				Multi-egress management	- Multi-egress links can be configured and managed, including NAT configuration and status monitoring on interfaces. 3G/LTE/5G links can function as standby links.

Level-1 Category	Level-2 Category	Level-3 Category	Level-4 Category	Item	Description
			Cloud-based modular switch management	-	Modular switches can be managed by the console. Basic O&M (diagnosis tool, performance monitoring, alarm reporting, and upgrade) and card insertion and removal are supported.
			Switch stacking	Stacking of fixed switches	• The console supports automatic stacking. • Tenant administrators can manage stacks and stack members. The console can display the alarm status of stacks, and allows users to onboard and disconnect stack master devices and stack members. • The console supports stack upgrade, certificate replacement, stack alarm management, performance monitoring, and device log reporting. • The console can deliver configurations to stack members, configure reserved VLANs, and perform multi-active detections for stacks.
				CSS of modular switches	• The console can manage CSSs set up by modular switches. It also allows users to view CSS topologies, inspect and upgrade CSSs, perform CSS split detections, and perform basic O&M operations for CSSs. • A member device in a CSS can be replaced.
			Network	Internet access	Two types of network configurations are supported: local Internet access and multi-branch interconnection.

Level-1 Category	Level-2 Category	Level-3 Category	Level-4 Category	Item	Description
				Network parameters	• Network configuration includes the name, description, purpose, VLAN ID, IP address, subnet mask, and DHCP configuration. The DHCP configuration includes the DHCP mode, DNS mode, server list in DHCP relay mode, IP address lease, and reserved IP address range. • Proxy ARP, MTU, management VLAN, and static management address policy configurations are supported.
				Static management IP address	Allows users to configure fixed management IP addresses of switch subnets, firewall subnets, and AR subnets.
			DHCP	-	When a terminal accesses the network through a NAT device, the following configurations need to be configured for the terminal: the DHCP address pool, IP address, mask, and IP address lease, primary WINS server, secondary WINS server, and static IP address.
			DNS	-	The DNS mode (client or relay agent), DNS server address list, and local domain name list can be configured.
			NAT	-	NAT in Easy IP mode can be configured.

Level-1 Category	Level-2 Category	Level-3 Category	Level-4 Category	Item	Description
			VPN	IPsec VPN (*)	• A VPN can be configured in hub-spoke and mesh modes when firewalls function as hub devices. • In hub-spoke mode, users can configure one hub site, configure an IKE proposal and an IPsec proposal through a security profile, and configure multiple spoke sites. The hub site can contain third-party or cloud managed devices, on which administrators can configure accessible VPN network segments. Spoke sites can contain any devices, devices in a selected scope, or third-party devices, on which users can configure accessible VPN network segments and VPN rate limit. • In mesh mode, multiple devices can connect to devices of the current site in mesh networking mode. Users can configure an IKE proposal and an IPsec proposal through a security profile, select all or specified devices at the current site to be added to the mesh network, and configure the accessible VPN network segments and VPN rate limit.

Level-1 Category	Level-2 Category	Level-3 Category	Level-4 Category	Item	Description
				IPsec VPN enhancement (*) NOTE This enhancement is applicable only to firewalls .	• Spoke sites support multiple uplinks in IPsec VPN intelligent traffic steering scenarios. – M spoke sites can connect to a hub site through N uplinks. Intelligent traffic steering rules are generated in a unified manner. – Intelligent traffic steering rules are re-generated when uplinks of a spoke site are changed. – Intelligent traffic steering rules are re-generated when a hub site is changed. • In the intelligent traffic steering scenario, link switchback is supported. Traffic is preferentially forwarded over the link with a higher priority. By default, the link with a higher priority is used. If the high-priority link is faulty, the link with a lower priority is used for traffic forwarding. After the high-priority link recovers, traffic is switched back to the high-priority link.
			Management VLAN	Management VLAN auto-negotiation of cloud managed devices	Cloud-managed devices support plug-and-play, and management VLAN auto-negotiation.
				Manual configuration of management VLANs	Users can configure management VLANs for intranet devices separately, so that the devices can obtain management IP addresses through these VLANs, preventing competition between management and service IP addresses.

Level-1 Category	Level-2 Category	Level-3 Category	Level-4 Category	Item	Description
				Management VLAN configuration	Wired and wireless PnP VLANs can be configured, and Layer 2 isolation policies can be configured for management VLANs based on ports of core switches.
				MSTP (*)	MSTP basic functions, such as spanning tree instances and region names, can be configured.
				RSTP (*)	RSTP can be enabled and RSTP priorities can be configured.
			Routing	Policy-based routing (PBR)	- Static PBR based on the 5-tuple information can be configured for route selection. - Dynamic PBR can be configured to implement intelligent traffic steering based on the application category and egress link quality.
				Configuring static routes for firewall sites	Static routes can be configured for firewall sites.
				Configuring static routes for switch sites	Static routes can be configured for switch sites.
				Configuring static routes for AR sites	Static routes can be configured for AR sites.
			CLI configuration tool	CLI configuration tool (*)	Traditional devices can be configured based on CLI configuration templates.

Level-1 Category	Level-2 Category	Level-3 Category	Level-4 Category	Item	Description
		WLAN service management	Configuration file management	Configuration file management (*)	Backup, comparison, and restoration of switch configuration files are supported.
			SSID management	SSID configuration	SSIDs can be created, modified, deleted, and viewed. Basic SSID configurations (including VLAN, maximum user count, radio enabling switch, SSID hiding, rate limiting, and WMM) and advanced SSID optimization configurations are supported.
				Terminal rate limiting by time range (*)	The functions of limiting uplink and downlink traffic rates on a single terminal by time range are supported.
			Radio management	-	- The console allows users to modify the country code, enable or disable radios, and set the frequency band, channel, transmit power, and gain of radios. - The console supports manual, automatic, and scheduled calibration of the 2.4 GHz and 5 GHz radios, and allows users to set a TPC threshold.
					Dual frequency bands can be enabled together on an AR with a built-in Wi-Fi module.
			Roaming	-	Layer 3 roaming between central APs and cloud APs is supported.
			WAC management	WAC basic configuration	- SSH reverse tunnels between the console and devices can be created through NETCONF. - Administrators can access device web systems through the console.

Level-1 Category	Level-2 Category	Level-3 Category	Level-4 Category	Item	Description
				Compatibility between APs of legacy models and WACs	The console can manage WACs and non-cloud managed APs, monitor the status of APs, and deliver configurations to WACs. The configurations that can be delivered to WACs are fewer than those of cloud APs.
				Association between WACs and Fit APs	Fit APs can be associated with and disassociated from WACs.
			Preventing interference from rogue APs (*)	-	Radio calibration policies can be configured to enable APs to automatically prevent interference from rogue APs.
			Load balancing (*)	-	APs can perform load balancing based on the number of terminals.
			Bluetooth (*)	Basic Bluetooth configuration (*)	Bluetooth broadcast and monitoring are supported.
				Personalized Bluetooth broadcast configuration (*)	Bluetooth broadcast parameters can be set to different values for devices at a site.

Level-1 Category	Level-2 Category	Level-3 Category	Level-4 Category	Item	Description
		QoS	Packet re-marking (*)	-	Packet re-marking is supported based on the IP subnet, protocol and port, host name, MAC address, application or application category (supported by APs, ARs, and firewalls, but not switches), user group, time range, and country and region (supported by firewalls).
			Rate limiting (*)	-	• Rate limiting is supported based on the IP subnet, protocol and port, host name, MAC address, application or application category (supported by APs, ARs, and firewalls, but not switches), user group, time range, and country and region (supported by firewalls). • Firewalls can rate-limit traffic based on the IP address. • SSID- and terminal-based rate limiting are supported for uplink and downlink traffic.
			Traffic shaping (*)	-	• Port queues and traffic shaping can be configured for device interfaces. • Device interfaces can be configured to trust DSCP and 802.1p (default) priorities.
			Congestion management (*)	-	Congestion management in PQ, WRR, DRR, and hybrid scheduling modes can be configured on interfaces.
		Basic security service management	Static MAC addresses binding (*)	-	Static binding entries among device MAC addresses, VLANs, and interfaces can be configured.

Level-1 Category	Level-2 Category	Level-3 Category	Level-4 Category	Item	Description
			Security policy (*)	Traffic policy	Devices compare traffic packet features with certain conditions and perform security control on the packets meeting the conditions.
			DHCP snooping	-	DHCP snooping can be configured on interfaces.
			MAC addresses blacklist and whitelist	-	The MAC address blacklist and whitelist can be configured.
			WIDS and WIPS (*)	-	- WIDS templates, whitelists (SSIDs, OUIs, and MAC addresses), and rules for identifying spoofing SSIDs can be configured. - WIDS detection can be configured to implement containment against unauthorized devices and clients. - Attack detection and defense can be configured.
			URL filtering	-	- Filters URLs based on predefined categories. - Filters URLs using the URL blacklist and whitelist (HTTP/HTTPS).
			Security signature database update (*)	Antivirus signature database update (*)	The console can update antivirus signature databases of firewalls.
				File reputation database update (*)	The console can update file reputation databases of firewalls.

Level-1 Category	Level-2 Category	Level-3 Category	Level-4 Category	Item	Description
				Malicious domain name database update (*)	The console can update malicious domain name databases of firewalls.
				IPS signature database update (*)	The console can update IPS signature databases of firewalls.
				IP reputation database update (*)	The console can update IP reputation databases of firewalls.
			Interference detection (*)	-	- Provides the function of detecting whether tenants suffer from interference. - Provides the functions of querying the interfered APs and interference types for tenants.
		Wireless non-operating management (*)	-	-	China's wireless access security requirements can be fulfilled.
	Network O&M	Monitoring	Alarm management	-	- Allows users to view device alarms. - Allows users to clear alarms.
			Device monitoring	Device state	The console can display devices in online, offline, unregistered, alarm, and faulty states.

Level-1 Category	Level-2 Category	Level-3 Category	Level-4 Category	Item	Description
				Device information	- Allows users to query details of a single device, including the device name, version, model, startup time, IP address, MAC address, running time, manufacturer, description, tag group, and location on the map. - Allows users to query information about interfaces on a device, including the interface running status, name, IP address, bandwidth, MTU, and duplex mode.
				Resource monitoring	- The console can monitor CPU and memory usages of a single device. - The console can display SSID and radio information about a single device. - The console can display traffic statistics and terminal information about a single device.
				AP air interface resource monitoring (*)	The console can display the statistics and trends of upstream and downstream unicast, multicast, and broadcast packets on air interfaces and wired interfaces of APs, as well as the status of those interfaces.
			Terminal monitoring	Online terminal information	Users can view the list of terminals that go online from a specified AP at a site. The terminal list contains diversified information, such as the terminal IP address, terminal MAC address, username, associated AP, negotiated rate, packet loss rate, signal-to-noise ratio (SNR), retransmission rate, signal strength, authentication mode, uplink and downlink rates, latest VLAN access time, access SSID, and traffic information.

Level-1 Category	Level-2 Category	Level-3 Category	Level-4 Category	Item	Description
				End user list export (*)	Exports end user lists within the last 30 days on the report customization page.
				Historical trend (*)	- Historical users in the past seven days can be viewed. - The console can display the quantity trend of terminals connecting to a site within a specified period of time, for example, one day, one week, one month, or one year.
				Mobility group and roaming neighbor	Information about roaming groups and roaming neighbors is reported periodically, and is displayed on the console. (in tables).
			Authenticated user monitoring (*)	-	- The console can display information about online users who pass Portal authentication. The information includes the username, user group, authentication mode, access policy, access SSID, terminal MAC address, terminal IP address, login time, and site. Online user information can be exported. - Tenant administrators can disconnect specific online users.
			Basic security service monitoring (*)	VPN status (*)	Allows users to query information about VPN tunnel connections, including the IPsec policy name, source device, source interface, destination device, and VPN status.

Level-1 Category	Level-2 Category	Level-3 Category	Level-4 Category	Item	Description
			Application monitoring (*)	Application identification (*)	- DPI can be configured on APs and firewalls to identify specific types of applications, for example, QQ, MSN, and Sina email box. - Through DPI application identification packets, statistics on traffic and application usages can be collected based on the time range, tenant, device, and site.
				DPI upgrade (*)	- Application data of the console can be updated online. - An upgrade address and an upgrade plan can be configured for firewalls, ARs, and APs. - The console can trigger a device to update application data online immediately. - The console supports application database upgrade in local mode. To implement this, tenants need to upload the database upgrade file to the console. The console can then deliver the file to devices for local upgrade of application data.

Level-1 Category	Level-2 Category	Level-3 Category	Level-4 Category	Item	Description
				Traffic analytics (*)	• The console can display the network traffic trend of all the devices at a site within the specified period of time, for example, one day, one week, one month, or one year. It can also display uplink and downlink network traffic trends. • The console can display top 5 devices by traffic at a site within the specified period of time, as well as the traffic statistics of each device. Users can click a device to view details. • The console can display top 5 SSIDs by traffic at a site within the specified period of time, as well as the traffic statistics of each SSID. • The console can display top 5 terminals by traffic at a site within the specified period of time, as well as the traffic statistics of each terminal. • Tenant-level statistics is supported.
			Application experience (*)	IP-based in-band flow measurement (*)	In-band flow measurement based on 5-tuple information is supported.

Level-1 Category	Level-2 Category	Level-3 Category	Level-4 Category	Item	Description
				Application-based in-band flow measurement (*)	• Identification of DPI applications and customized applications is supported. The functions of collecting and reporting application traffic statistics are supported. • The console can display switch traffic statistics of a single application and of applications in an application list, and can also display top N applications by traffic. • Application-based in-band flow measurement is supported.
				-	• Supports automatic discovery and display of physical topologies. • Displays status of and basic information about devices. • Supports quick search for devices. • Allows users to view networking traffic heatmaps.
		Topology management	Site network topology	-	• Displays VPN connection information between sites on a GIS map. • Displays VPN tunnel status.
			GIS topology	-	• Displays VPN connection information between sites on a GIS map. • Displays VPN tunnel status.
		Fault diagnosis	Remote CLI login (*)	-	Users can remotely log in to the CLI of devices on the console to diagnose device faults. Firewalls support this function in V300R003C00 and later versions.
			Remote control (*)	-	• Allows users to blink an AP indicator. • Allows users to remotely restart devices on the console. • Allows users to turn on or off AP indicators in a specified time period.

Level-1 Category	Level-2 Category	Level-3 Category	Level-4 Category	Item	Description
			Batch device restart (*)	-	Users can select multiple devices and restart them in batches with one click, simplifying O&M and quickly recovering services.
			Packet header obtaining (*)	-	Users can configure packet header obtaining (obtaining 64 bytes of a packet) on specific device ports on the console. Users can also download the obtained packets from the console.
			Packet path tracing (*)	-	Packets of the following protocols can be detected: ICMP, IGMP, IP-in-IP, TCP, UDP, GRE, and OSPF.
			Diagnosis information collection (*)	-	Allows users to manually collect device diagnosis information, and automatically collect diagnosis information of a device when the device's CPU usage or memory usage is high or the device restarts.
			Fault locating (*)	Fault locating method	Allows users to view rogue signals based on APs on the console.
				Fault locating tools	The following tests are supported: ping test, traceroute test, radio ping test, and virtual cable test.
		Network quality analysis	SLA management (*)	-	SLA management is supported for traditional devices.

Level-1 Category	Level-2 Category	Level-3 Category	Level-4 Category	Item	Description
		Upgrade (*)	Software package management (*)	-	• SLA management is supported for traditional devices. • Allows users to upload, modify, delete, and query software packages and patches. • Allows users to download device software packages from the Huawei Online Upgrade Repository (HOUP).
			Software upgrade (*)	-	• Users can install software packages and patch files by site, and view the installation progress. The console supports automatic upgrade for devices running earlier software versions. When a device is added to the site with devices running a later software version, the console automatically upgrades the newly added device to the later version. • Users can select the desired devices for upgrade. • The console supports the version upgrade of cloud managed devices at a site. • The console supports the upgrade of traditional devices (through uUpgrade). • The console supports the upgrade of stacks set by cloud managed devices.
			Resumable transfer (*)	-	Resumable transfer is supported for software packages during upgrade.
			Time window (*)	-	Users can configure the upgrade time window. When the time window starts, the device upgrade begins, and the upgrade stops till the end of the time window.

Level-1 Category	Level-2 Category	Level-3 Category	Level-4 Category	Item	Description
		Reports (*)	Statistics report (*)	-	• The following statistics are collected by tenant or site: – Total uplink and downlink traffic statistics at the site egress (from the site perspective) and total traffic statistics of each site (from the tenant perspective) – Number of access clients (access terminals) every day under a tenant or at a site. Users can configure the console to display top N records (N is configurable). – Traffic statistics of each SSID, AP, user/user group, and application category/application under a tenant or at a site. Users can configure the console to display top N items (N is configurable). – Security events (WIDS/IPS analysis and network alarms) under a tenant or at a site can be exported. Top N tenants can be displayed. • Reports can be periodically exported in CVS or other formats, by day, week, month, or year, and can be sent via emails.

Level-1 Category	Level-2 Category	Level-3 Category	Level-4 Category	Item	Description
			Agile report (*)	-	• The console provides a default scenario-specific dashboard to simplify O&M, and allows users to flexibly customize dashboards based on their O&M requirements. The console also supports orchestration of common data sources and correlative data analysis. Analysis reports can be periodically exported to Word, PDF, or CSV files. • The following reports are available based on the agile report framework: – Resource reports: device vendor, device type, and device model reports – Authentication reports: online terminal trend chart, online user trend chart, RADIUS log statistics chart, Portal log statistics chart, terminal type proportion chart, top N terminals by vendor, and top N terminals by OS.
		Logs (*)	Device channel logs (*)	-	Generates logs when the configuration channels, performance channels, authentication channels, and IP-security group channels are set up, and allows users to query these logs.
			Onboarding and disconnection logs of authenticated users (*)	-	The console can display onboarding and disconnection logs of Portal authentication users. Such a log contains the following information: username, authentication time, terminal MAC address, terminal IP address, disconnection time, authentication mode, user type, authentication failure cause, and associated SSID. These logs can be exported.

Level-1 Category	Level-2 Category	Level-3 Category	Level-4 Category	Item	Description
			Unified device log management (*)	-	The console can collect and display AP logs and allows users to export logs and delete expired logs.
			Centralized log management (*)	-	• An independent syslog server can be configured for a tenant. The following logs can be reported: operation logs, security logs, and onboarding and disconnection logs of clients and devices. SSL encryption is supported. • Syslog servers can be configured for APs, WACs, switches, firewalls, and ARs on the console.
	Network health 360	Dashboard	-	-	Displays the evaluation results of the entire network, including the health scores, number of access users, number of devices, traffic statistics, network-wide issue distribution, number of times calibration is performed, inter-generation AP upgrade, and decision-making items for coverage hole compensation.

Level-1 Category	Level-2 Category	Level-3 Category	Level-4 Category	Item	Description
		Wireless network health	-	-	• Three-level evaluation results (excellent, good, and poor) are provided based on the following metrics: access success rate, access time consumption, roaming fulfillment rate, signal and interference, capacity health, and throughput fulfillment rate. • Root causes are analyzed based on the following metrics: association/authentication/DHCP success rate, time required for association/authentication/DHCP, signal strength, channel utilization, number of users, bandwidth, roaming success rate, roaming duration, interference rate, air interface congestion fulfillment rate, and non-5G-prior access. • Users can view metric rankings and trends, root causes of issues, and details about metrics. • Data analytics supports the following capabilities to improve operation efficiency: – Associated issue display – Data clustering by AP, user, and SSID – Identification of faulty terminals and APs • Users can download health evaluation reports to local hosts.

Level-1 Category	Level-2 Category	Level-3 Category	Level-4 Category	Item	Description
		Issue analysis	-	-	- Allows users to view the number, distribution, and details of connectivity issues. Connectivity issues include authentication failure (802.1X authentication and MAC address authentication), slow authentication (802.1X authentication), authentication timeout (802.1X authentication and MAC address authentication), association failure (not supported for wired clients), slow association (not supported for wired clients), DHCP failure, and slow DHCP. - Identifies the root causes of the following issues: issues that the authentication server is unreachable, issues that the number of clients exceeds the capacity, authentication issues, and associated device issues. NOTE Due to differences between Portal servers and inconsistent Network Admission Control (NAC) processes, a Portal server must work with a RADIUS authentication server to implement Portal authentication. - Allows users to view the number, distribution, and details of air interface performance issues, including weak-signal coverage, high channel utilization, high interference, air interface congestion, client capacity, and non-5G-prior access. - Allows users to view the number, distribution, and details of roaming issues, including repeated roaming.

Level-1 Category	Level-2 Category	Level-3 Category	Level-4 Category	Item	Description
	User experience 360	Client list	-	-	Allows users to view client access information lists.
		Client journey	-	-	Allows users to view client journey information, including client information, metric overview, and details about each node.
		Protocol tracing	-	-	Wireless client access phases including association, authentication (supporting only the 802.1X authentication mode), and DHCP are displayed in terms of different protocols. Refined analysis for individual faults that occur during client access is provided based on the protocol interaction result and duration at each phase. The analysis includes the most possible root causes and rectification suggestions for client access failures.
	Intelligent optimization 360	Homepage overview	-	-	- Allows users to view optimization benefits, including the uplink and downlink bandwidth, channel utilization, and interference rate. - Allows users to view AI roaming benefits, including the roaming success rate, signal strength before roaming, and bandwidth during roaming. - Allows users to view AI inference data, including the number of high-load APs, number of edge APs, number of key APs, number of roaming terminal profiles, and number of terminal vendors. - Allows users to view the number of times intelligent radio calibration and AI roaming steering are performed.

Level-1 Category	Level-2 Category	Level-3 Category	Level-4 Category	Item	Description
		AI inference	-	-	- Allows users to view details about high-load APs. - Allows users to view details about edge APs. - Allows users to add, delete, and view key APs.
		Calibration records	-	-	Allows users to view calibration records, including the calibration duration, calibration type, calibration scope, frequency band, uplink and downlink bandwidth of terminals after calibration, interference rate, and channel utilization.
		AI roaming	-	-	- Supports AI roaming terminal statistics, including the number of trained terminal profiles and number of times roaming steering is performed. - Allows users to view AI roaming steering data by vendor, including the vendor, number of profiles of different models under each vendor, number of terminals, number of roaming steering successes, signal strength before roaming, and uplink and downlink rates. - Allows users to view AI roaming details, including roaming terminals, roam-out and roam-in APs, and roaming details.
	Application assurance 360	Application overview	-	-	- Allows users to view the application list, invalid applications, and traffic statistics, ensuring application visibility. - Analyzes total traffic trends at a site and sets thresholds to monitor traffic.

Level-1 Category	Level-2 Category	Level-3 Category	Level-4 Category	Item	Description
		Network traffic analysis	-	-	Analyzes network traffic by device and host.
Cloud-based admission	User management (*)	Local user management (*)	User management (*)	-	- Allows users to create, modify, and delete user information, including the username, password, email address, expiration time, and contact number. The information is used for Portal authentication. - Allows users to import and export the user information. - Allows users to register accounts by themselves.
			User group management (*)	-	- Allows users to create, modify, and delete user group information, including the user group name, address, postal code, administrator email address, and description. User group information is used in access control policies. - Allows users to import and export user groups (using the same template for user import and export).
		Guest management (*)	Guest account management (*)	-	- Allows tenant administrators and guest administrators to create common guest accounts, which can be cleared periodically. - Allows tenant administrators to create passcode accounts in batches. - Allows guest administrators to manage guest accounts by group or role. - Sends account expiration notifications via emails or SMS messages.

Level-1 Category	Level-2 Category	Level-3 Category	Level-4 Category	Item	Description
			Guest account policy (*)	-	• The guest username can be an account name, a mobile number, an email address, or a public QR code. • Policies for enabling and approving guest accounts, as well as notification policies, can be configured. • Guest login types can be restricted.
			Guest account approval (*)	-	• Guest accounts can be approved in the following modes: approval-free, tenant administrator approval, employee approval, email-based approval, and public QR code-based approval. • Approval notifications can be sent via SMS messages or emails. • Messages that indicate successful guest account approvals can be sent via SMS messages or emails, or displayed on web pages.
			Guest authentication (*)	-	The following authentication modes are applicable to guests: username and password authentication, passcode authentication, SMS authentication, two-factor authentication, anonymous authentication, URL-based WeChat authentication, Wi-Fi via WeChat authentication, social media authentication (Facebook, Twitter, QQ, and Sina Weibo), WeChat authentication in developer mode, and public QR code authentication.
			Guest account application method (*)	-	Currently, guest accounts can be created by tenant administrators (one by one or in batches), be created by guest administrators (one by one or in batches), and be applied for by guests on their own.

Level-1 Category	Level-2 Category	Level-3 Category	Level-4 Category	Item	Description
			Configuration wizard for guest management functions (*)	-	The console provides a wizard for helping users to configure guest management functions, simplifying system deployment and implementation.
		Interconnection with a third-party data source (*)	Social media authentication (*)	-	Facebook and Twitter accounts can be used for social media authentication.
		Online user management (*)	Online user management (*)	-	Online users can be disconnected, and their data can be exported. RADIUS CoA authorization information can be changed through HACA channels.

Level-1 Category	Level-2 Category	Level-3 Category	Level-4 Category	Item	Description
		Traffic volume and online duration control (*)	Traffic volume and online duration control (*)	-	User/Terminal traffic volume and online duration statistics collection and management: • User/Terminal traffic volume limit • User/Terminal online duration control • Terminal one-time online duration limit • User/Terminal traffic volume and online duration limits based on user groups • Manual clearance of user/terminal online duration information • Manual reset of user/terminal traffic volume information • Periodic clearance of online user/terminal traffic volume information • Automatic reset of user/terminal traffic volume and online duration information upon each login • User/Terminal traffic volume and online duration statistics collection
	Terminal management	Terminal management (*)	Terminal and terminal group management (*)	Terminal and terminal group management (*)	• Terminal groups can be created, deleted, modified, and queried, and can be nested. • The console can add terminals that are automatically discovered to terminal groups, and also allows users to manually add terminals and add them to terminal groups. • The console allows access of identified terminals and supports the terminal blacklist function. • The console allows users to configure policies for identifying preset terminals and custom terminals.

Level-1 Category	Level-2 Category	Level-3 Category	Level-4 Category	Item	Description
				Camera terminal management (*)	In addition to the terminal management functions, the following functions are newly supported: - Allows users to check the PoE status of interfaces connecting to cameras and enable/disable the interfaces. - Allows users to view camera traffic information.
				Terminal identification (*)	- Rule database: Fingerbank - Identification methods: User-Agent, DHCP Option, MAC OUI, mDNS, and LLDP - Terminal information that can be identified: OS, vendor, terminal model, and terminal type
				AI clustering/identification (*)	- Unknown terminals are classified by type to facilitate unified processing by administrators. - Unknown terminals can be identified automatically based on learned marking rules.
				Offline update of the terminal fingerprint database (*)	Allows users to update the built-in terminal fingerprint database of the console by importing a new terminal fingerprint database.
			5G terminal access (*)	-	5G IoT terminals can access campus networks.

Level-1 Category	Level-2 Category	Level-3 Category	Level-4 Category	Item	Description
			IoT aware network (*)	-	- SSIDs specific to iConnect terminals are configured to implement plug-and-play of iConnect IoT terminals. - iConnect terminals can automatically load digital certificates to enhance access security.
		Terminal authentication logs (*)	Portal user login and logout logs (*)	-	Login and logout logs of Portal users can be filtered, viewed, and exported.
			RADIUS user login and logout logs (*)	-	Authentication and accounting logs of RADIUS users can be filtered, viewed, and exported.
		Boarding management (*)	Boarding management (*)	-	Allows users to configure 802.1X authentication and manage network access policies through Boarding clients.
	Portal authentication	Built-in Portal authentication (*)	Portal protocol (*)	-	The console supports HTTP/2-based HACA Portal authentication (bypass supported).
			MAC prioritization (*)	-	- The console saves MAC addresses of terminals, so that users can directly access networks using the terminals without entering usernames and passwords. - Cross-site MAC address-prioritized Portal authentication is supported.

Level-1 Category	Level-2 Category	Level-3 Category	Level-4 Category	Item	Description
			Authentication mode (*)	-	The following Portal authentication modes are supported: username and password authentication, anonymous authentication, SMS authentication, Facebook authentication, and passcode authentication.
		Username and password generation policy (*)	Batch generation of usernames and passwords (*)	-	Accounts can be created in batches, and the validity period of the accounts can be specified. The validity period starts from the time when a user is authenticated for the first time.
			One-click generation of usernames and passwords (*)	-	Generates login passwords of accounts with one click.
			Passcode (*)	-	Allows users to be authenticated by entering only one parameter.
		Control over the number of access terminals (*)	-	-	The number of terminals using the same account to access a network is limited in username and password Portal authentication.

Level-1 Category	Level-2 Category	Level-3 Category	Level-4 Category	Item	Description
		Interconnection with a third-party Portal server (*)	-	-	• The console can interconnect with a third-party Portal server and deliver interconnection parameters with the third-party Portal and RADIUS servers. • APs can interconnect with a Srun server that function as a third-party Portal server. Firewalls can interconnect with the campus controller.
		Portal page management (*)	Page customization (*)	-	• Preset Portal page templates, and dial-up and carousel image controls on Portal pages are supported. Users can add and delete Portal pages based on the templates, as well as modify the logo, title, description, and style of pages. • Preset pages: URL-based WeChat authentication page, username and password authentication page, SMS authentication page, passcode authentication page, one-click authentication page, social media authentication page, anonymous authentication page, and full-screen advertisement page • Portal pages can be customized.
			Portal page language (*)	-	The language in which Portal pages are presented can be set to English, Germany, or Spanish.
			Portal management (*)	-	Allows users to upload Portal pages and delete Portal files.

Level-1 Category	Level-2 Category	Level-3 Category	Level-4 Category	Item	Description
			Portal page push policy (*)	-	Different Portal pages can be pushed based on conditions specified in Portal page push policies. The following conditions can be configured: device, device type, device group, terminal OS, browser language, terminal IP address, SSID, time, and site.
	PPSK/DPSK	PPSK/DPSK (*)	-	-	- PPSK accounts can be configured on the console web UI. The console provides APIs for configuring PPSK accounts, and allows users to import and export PPSK accounts in batches. - Different PSK passwords can be provided for different users.
	Social media authentication	WeChat authentication (*)	URL-based WeChat authentication mode (*)	-	A URL can be provided for WeChat authentication. This mode requires a URL access key.
			QR code-based WeChat authentication (*)	-	Users can be authenticated after scanning QR codes provided by the WeChat official accounts they have followed.
		Facebook authentication (*)	-	-	Users can be authenticated by entering their Facebook usernames and passwords.

Level-1 Category	Level-2 Category	Level-3 Category	Level-4 Category	Item	Description
		Twitter authentication (*)	-	-	Users can be authenticated by entering their Twitter usernames and passwords.
	SMS authentication	SMS authentication (*)	-	-	SMS authentication and preset Twillio and fungo SMS templates are supported.
		SMS content customization (*)	-	-	Allows users to customize the content of SMS messages used for authentication.
	RADIUS authentication	RADIUS server (*)	-	-	The console can function as RADIUS authentication and accounting servers.
		RADIUS proxy (*)	-	-	The console can interconnect with a third-party authentication server and an accounting server using the RADIUS protocol.
	Authentication rule management	Conditions in authentication rules (*)	-	-	The following conditions and their combinations can be configured in authentication rules: user, user group, role, site, admission device group, device type, access device, SSID, terminal group, terminal IP address, address range, time range, customized conditions based on RADIUS attributes, authentication mode, and access mode.

Level-1 Category	Level-2 Category	Level-3 Category	Level-4 Category	Item	Description
		Authentication rule processing (*)	-	-	• The console supports self-learning of the IP address, access VLAN, and access port of an access device, MAC address and IP address of an access user, and IMSI and SN of a terminal. • If an account has no access information bound, the account is not allowed to access the network. • Multiple data sources can be specified in authentication rules. • The preferred protocol for 802.1X authentication can be configured on the server side to increase the protocol negotiation rate. • In RADIUS authentication scenarios, the RADIUS protocol types supported on the server side can be restricted. • If a user does not exist, three policies can be executed: continue processing, not send response packets, and deny access. • When identity authentication fails, three policies can be executed: continue processing, not send response packets, and deny access.
	Authorization result management	Conditions in authorization rules (*)	-	-	The following conditions and their combinations can be configured in authentication rules: user, user group, role, site, admission device group, device type, access device, SSID, terminal group, terminal IP address, address range, time range, customized conditions based on RADIUS attributes, authentication mode, and access mode.

Level-1 Category	Level-2 Category	Level-3 Category	Level-4 Category	Item	Description
		Authorization result management (*)	-	-	The following authorization results can be configured: authorization VIP user identity, authorization URL filtering, authorization ACL, authorization VLAN, authorization QoS, authorization application scheduling (HQoS), user-defined RADIUS authorization parameters, authorization security group, authorization redirection, ACL (dynamic ACL and static ACL), and pushed authorization URL.
	Admission configuration delivery	Authentication configuration delivery management (*)	Authentication configuration for cloud APs (*)	-	Cloud APs support Portal authentication, PSK/PPSK authentication, MAC address authentication, and 802.1X authentication.
			Authentication configuration for switches (*)	-	- Wired and wireless access authentication for switches include Portal authentication, PSK/PPSK authentication, MAC address authentication, and 802.1X authentication. - The wired access mode on switches can be specified as follows: - An interface can allow access of multiple terminals or only one terminal. - Multiple terminals are authenticated separately, and only the first terminal needs to be authenticated.

Level-1 Category	Level-2 Category	Level-3 Category	Level-4 Category	Item	Description
			Authentication configuration for firewalls (*)	-	Firewalls support Portal authentication.
			Authentication configuration for ARs (*)	-	ARs support Portal authentication.
		Authorization configuration delivery management (*)	Cloud AP authorization configuration (*)	-	The following authorization configurations can be configured on cloud APs: VIP user, ACL, URL filtering, terminal traffic rate limiting, DSCP, and VLAN.
			Switch authorization configuration (*)	-	The following authorization configurations can be configured on switches: VIP user, ACL, IPv6 ACL, security group, VLAN, terminal traffic rate limiting, and application control template.
			Firewall authorization configuration (*)	-	The security group can be configured on firewalls.
			AR authorization configuration (*)	-	The following authorization configurations can be configured on ARs: ACL, terminal traffic rate limiting, and DSCP.

Level-1 Category	Level-2 Category	Level-3 Category	Level-4 Category	Item	Description
		PPSK account delivery (*)	-	-	PPSK account delivery is applicable only to APs.
	Free mobility	Free mobility resource management	Security group management	-	• The console can manage security groups, including bypass security groups. • Security groups can be imported and exported.
			Resource group management	-	• The console supports resource group management. • Resource groups can be imported and exported.
		Free mobility policy	Free mobility policy	-	The following free mobility policy configurations are supported: • Policy matrix specific to a site • Policy matrix specific to a fabric network • Policy matrix modification • Policy matrix deployment • Inter-group access control policy • Group policy configuration in batches • Reverse policy configuration • Inter-group policy display in a matrix or list • Custom policy view • Policy priority adjustment
	IPv6 user authentication	802.1X authentication (*)	-	-	IPv6 terminals can access campus networks after passing 802.1X authentication.

Level-1 Category	Level-2 Category	Level-3 Category	Level-4 Category	Item	Description
		MAC address authentication (*)	-	-	IPv6 terminals can access campus networks after passing MAC address authentication.
		Portal authentication (*)	-	-	IPv6 terminals can access campus networks after passing Portal authentication.
SD-WAN (*)	Network configuration	Network planning configuration	Physical network	-	Parameters for physical networks: routing domain, transport network, IPsec encryption, device activation security, link connectivity detection, intelligent traffic steering, and NTP configurations
			Virtual network	-	Parameters for virtual networks: routing, IP address pool, DNS, and port configurations
			Collection configuration	-	Parameters for statistics collection: application traffic, application quality, and WAN link traffic
		WAN physical network	Physical interface	-	Physical interfaces and Eth-Trunk interfaces can be configured.
			ZTP	-	WAN-side links and NTP can be configured for a site. Multiple deployment modes are supported, including email-, USB-, and DHCP option-based deployment.
			WAN route	Static routing protocol	The CPE gateway can communicate with the WAN through IPv4 and IPv6 static routing protocols.
				OSPF	The CPE gateway can communicate with the WAN through OSPF.

Level-1 Category	Level-2 Category	Level-3 Category	Level-4 Category	Item	Description
				BGP	The CPE gateway can communicate with the WAN through BGP and BGP4+.
			VLAN	-	VLANs can be configured to implement Layer 2 isolation, so as to enhance network security.
			Interconnection between non-SD-WAN sites	GRE	IPv6 packets are encapsulated into IPv4 packets through GRE tunneling technology, so that IPv6 packets can be transmitted on IPv4 networks. This enables IPv6 branches to communicate with each other.
				IPsec	SD-WAN sites can set up IPsec tunnels with legacy sites, third-party sites, or public cloud VPCs.
			Universal configuration	TACACS	A TACACS server can be configured.
				Authentication mode	NAC authenticates access clients and users on the LAN side to ensure network security.
				Advanced device configuration	The device QoS mode and QoS GTS can be configured.
				Connection source port	A source port can be configured for STUN connections.
				Local TNP-preferred traffic steering	Local TNP-preferred traffic steering can be configured.
				Device reliability	VRRP MAC types can be configured.
			RR connection	-	Associates edge sites with route reflector (RR) sites.

Level-1 Category	Level-2 Category	Level-3 Category	Level-4 Category	Item	Description
		WAN virtual network	Topology	-	The topology model for inter-site communication varies according to service communication requirements. • Predefined topology – Single-layer network models: hub-spoke, full-mesh, and partial-mesh – Hierarchical network model: Multiple areas are interconnected through a centralized hub area (backbone area) so that a large number of sites can communicate with each other across areas. • Customized topology – Topology policies can be customized based on the predefined topology to adjust the interworking paths between sites.
			LAN interface	-	Layer 3 and Layer 2 interfaces can be configured for CPE gateways at sites to connect to the LAN.
			LAN route	Static routing protocol	The CPE gateway can communicate with the LAN through IPv4 and IPv6 static routing protocols.
				OSPF	The CPE gateway can communicate with the LAN through OSPF and OSPFv3.
				BGP	The CPE gateway can communicate with the LAN through BGP and BGP4+.

Level-1 Category	Level-2 Category	Level-3 Category	Level-4 Category	Item	Description
			WAN route	WAN routing policy	- After the overlay network is configured, the system automatically deploys BGP between sites to advertise routes on the overlay network. - Blacklist and whitelist can be configured for overlay route filtering to filter the BGP routes to be advertised or received on the overlay WAN side.
				WAN routing policy template	Allows users to configure and modify WAN routing policies in batches through configuring a WAN routing policy template.
			WLAN	-	The WLAN can be configured so that wireless terminals on the LAN side can access gateways through Wi-Fi.
			Loopback interface	-	Overlay loopback interfaces can be configured in an overlay VPN network.
			Static ARP	-	Static ARP entries can be configured based on IPv4.
			VAS connection	-	CPEs connect to the firewall through the VAS connection function. The firewall functions as a centralized security gateway to protect traffic from headquarters and branches.
	Application experience	Security policy	URL	-	URL security policies can be configured to control the URLs that users can access.
			Firewall	-	Firewall security policies can be configured to logically separate an internal network from an external network. This implements security protection for Internet access services of users and protects the internal network from unauthorized external access.

Level-1 Category	Level-2 Category	Level-3 Category	Level-4 Category	Item	Description
			IPS and AV	-	A policy can be configured to implement the intrusion prevention system (IPS) and antivirus (AV) functions. After the policies are applied to a device, the device compares characteristics of received packets against the preset IPS and virus signature databases. If a match is found, the device takes the corresponding prevention measure.
		Traffic policy	Overlay QoS	-	The bandwidth of applications or traffic can be limited
			Overlay ACL	-	An ACL policy can be deployed on the LAN side to block specific traffic between internal users and external networks.
			Intelligent traffic steering	-	When there are multiple links to the destination network, intelligent traffic steering enables devices to dynamically select the optimal link based on the link quality, bandwidth, and application priority. By monitoring the network quality in real time, devices dynamically adjust traffic forwarding paths based on the real-time status of each link. This minimizes the impact of network quality on user experience.
			WAN optimization	-	Technologies such as forward error correction (FEC), multi-fed and selective receiving, and per-packet load balancing improve the quality and efficiency of data transmission over WAN links.
			Site-to-Internet access	-	The local Internet access, centralized Internet access, and hybrid Internet access are supported.

Level-1 Category	Level-2 Category	Level-3 Category	Level-4 Category	Item	Description
			Site-to-legacy networking	-	The local access, centralized access, and hybrid access are supported.
			Overlay NAT	-	Dynamic NAT can be implemented in three modes: Easy IP, PAT, and No-PAT.
			Underlay ACL	-	An ACL policy can be configured on the WAN side to prevent specific traffic from external networks from entering CPEs and internal networks.
			Cloud security	-	Security policies can be configured for interconnection with a third-party cloud security gateway, so as to enhance Internet access security.
			Underlay NAT	-	Allows intranet users with private IP addresses to access public IP addresses on public networks.
			Common QoS	-	When service packets are sent from the LAN side to the WAN side on the underlay network, the common QoS is recommended to limit the bandwidth of applications or traffic.
			NAT ALG	-	NAT can be performed for specific application-layer protocols.
			Dynamic QoS	-	Relieves congestion for key service assurance.
			Redirection	-	Redirection policies can be configured on EVPN tunnel interfaces, interworking tunnel interfaces, and LAN interfaces.
			Broadcast packet forwarding	-	Enables a device to receive and forward directed broadcast packets.

Level-1 Category	Level-2 Category	Level-3 Category	Level-4 Category	Item	Description
		Application management	Customized application	-	The console can identify traffic of common applications using its built-in application signature database. When predefined applications cannot meet the requirement, users can create such applications based on their signatures. There are three application types: SA, Domain Name, and Advance Rule.
			Application group	-	Allows users to create an application group to match application traffic to be identified.
	Network monitoring	WAN site interconnection	Link traffic	-	- Allows users to view the link traffic distribution chart and top 10 applications by traffic. - Allows users to view the throughput trend, bandwidth usage trend, and LQM trend by time range.
			Link quality	-	Allows users to view link quality data, including the LQM trend, delay change trend, jitter change trend, and packet loss rate change trend.
			SPR switch over	-	Allows users to view the SPR switchover statistics of the selected site.
			Application	-	Allows users to view the application quality and the quality of the link where the application traffic is forwarded, throughput trend, and uplink and downlink bandwidth usage trend.
			FEC	-	Allows users to view the optimization effect after WAN optimization.
		Application monitoring	-	-	Allows users to view application information, application AQM, statistics ranking, details about applications between network-wide sites, and performance trends.
	(*): The feature needs to be operated on the GUI of iMaster NCE-Campus.				

1.2 Border Protection and Response

Table 1-2 Specifications

Level-1 Category	Level-2 Category	Item	Description
Management	Security situation dashboard	Compromised asset situation	Includes the compromised host trend, compromised host distribution, compromise event blocking rate, latest compromise events, top compromised hosts, top compromise types, and top compromise events.
		Basic security event situation	Includes the attack location, average threat detection duration, blocking rate, top attack types, latest threat events, and number of special events.
		External attack source situation	Includes the external attack source trend, attack source distribution, external attack blocking rate, latest external attacks, top attack sources, attack assets, and attack types.
	Periodic security report	Periodic security report	Sends security service reports to users' subscription mailboxes by week or month. Security service reports enable customers to clearly understand the following information: 1. Overview of security service. 2. Threat prevention times and trend. 3. Number and details of compromised hosts. 4. Number and trend of external attack sources. 5. Number and trend of malicious files. Supports statistics collection of application access based on the source IP addresses, access time, and application distribution, and provides statistical analysis reports by week or month. 1. Allows users to view and preview historical security reports. 2. Allows users to download reports.

Level-1 Category	Level-2 Category	Item	Description
	Security zone management	Security zone status management	1. Monitors the security zone status and checks whether physical connections in the security zone are reversely connected. 2. Sets trust labels for security zones.
	MSSP	MSSP-managed O&M	Creates an agency relationship for security services on the user O&M platform and creates roles (such as administrators and auditors) with different operation permissions for the delegated parties. After the agency relationship is established, the delegated party can check and handle security threat events.
		MSSP security dashboard	Displays threats for tenants managed by the MSSP.
		MSSP ticket transfer	Transfers tenants' tickets to the MSSP for analysis and handling.
Protection	Qiankun Shield/Firewall threat prevention	Malware protection	Supports multi-level protection technologies, detects multiple types of malicious code carriers, and updates the antivirus database in real time to cover popular high-risk malware. Note: Devices of 1 U high and desktop devices support a virus database containing 5 million viruses and 3 million viruses, respectively.
		Defense against botnets, Trojan horses, and worms	Supports precise role identification based on the botnet topology analysis technology; identifies 500+ botnets as well as 1000+ worms and Trojan horses.
		Service awareness	Identifies over 6000 applications and covers all mainstream application protocols.
		Web category	Supports a web category database with more than 120 million websites to regulate access behaviors and prevent malicious websites from attacking enterprise networks.

Level-1 Category	Level-2 Category	Item	Description
		Intrusion prevention	Supports attack detection technologies based on vulnerability and behavior analysis, anti-evasion technologies based on content restoration in context, a signature database containing more than 12,000 signatures, and automatic signature database update. Devices of 1 U high and desktop devices support a signature database containing 12,000 and 5000 signatures, respectively. Both of them support botnet detection and application server protection.
Response	Manual blocking	Manual blocking	Manually blocks the attack source based on the detected external attack source events.
	Automatic threat blocking	Automatic blocking of external attack sources	Accurately identifies external high-risk attack sources and automatically blacklists them to prevent subsequent attacks.
		Automatic blocking of malicious domain names	Automatically blocks malicious domain names based on DNS filtering to block the access of hosts on the user network to malicious domain names.
	Emergency security notification	SMS notification	Supports emergency notifications via SMS to notify users of threat events and provides timely response guidance.
		Email notification	Supports emergency notifications via email to notify users of threat events and provides timely response guidance.
		Alarm templates	Enables operations personnel to customize alarm templates for critical alarms that need to be sent to users.
	Blacklist and whitelist	Domain name blacklist	Configures a domain name blacklist to block access of hosts on the user network to malicious domain names.
		Device blacklist	1. Allows users to set blacklists to quickly block threat attack sources. 2. Allows users to view historical device blacklists. 3. Supports one-click clearance.

Level-1 Category	Level-2 Category	Item	Description
Analysis		Protected network segment	Supports association with protected network segments to protect existing services from being incorrectly blocked.
		Tenant global whitelist	Allows tenants to set a global whitelist to protect existing services and prevent them from being incorrectly blocked.
		Device whitelist	Allows tenants to set device whitelists to protect existing services. Content security detection will not be performed on whitelisted addresses.
	Special event analysis	Compromised hosts	Performs automatic aggregation as well as quick analysis and handling based on compromised hosts.
		External attack sources	1. Supports automatic aggregation by external attack sources, and performs quick analysis and handling by external attack sources. 2. Exports external attack sources.
		Malicious files	Performs automatic aggregation as well as quick analysis and handling based on malicious files.

1.3 Huawei Qiankun App

Table 1-3 Specifications

Level-1 Category	Level-2 Category	Item	Description
DFX	Privacy protection	Sensitive information anonymization on UIs	1. Anonymizes the phone number and email address in personal information of a tenant. 2. Anonymizes information such as the name, phone number, email address, and WeChat ID in a tenant's namecard and displays the real information when the tenant taps them.

Level-1 Category	Level-2 Category	Item	Description
		Privacy agreement signing and display	Allows users to view the latest privacy statement and customer agreement of Huawei Qiankun.
Security scenario homepage	Recommendations for security scenarios	Border protection and response service introduction page	Allows users to quickly view the introduction of the Huawei Qiankun border protection and response service.
	Security health score display	-	Allows users to view security health scores.
	Security device list	-	1. Allows users to view security devices (Qiankun Shield and firewalls). 2. Allows users to create, delete, modify, and query security devices. 3. Allows users to query devices by page. A maximum of 10 devices are displayed on each page.
	Quick entry to asset services	Asset management	Allows users to create, delete, modify, and query assets, filter assets by type, and follow assets with one click.
	Barcode scanning-based deployment	Firewall deployment	Supports barcode scanning-based deployment of firewalls on the Huawei Qiankun Cloud Platform.
		Qiankun Shield deployment	Supports barcode scanning-based deployment of Qiankun Shield devices on the Huawei Qiankun Cloud Platform.
	Quick entry to security services	Automatic blocking rate of security events	Allows users to view the automatic threat blocking rate in the border protection and response service.

Level-1 Category	Level-2 Category	Item	Description
		Blacklist and whitelist	Delivers blacklists and whitelists of Qiankun Shield devices using the border protection and response service.
		Security report	1. Supports export and sharing of weekly and monthly security reports with simply one tap in the border protection and response service. 2. Allows users to share security reports on WeChat Moments and to WeChat friends. 3. Allows users to export security reports generated in the last two months.
		Malicious files	Allows users to view and quickly handle malicious file events in the border protection and response service.
		Compromised hosts	Allows users to view and quickly handle compromised host events in the border protection and response service.
		External attacks	Allows users to view and quickly handle external attack events in the border protection and response service.
	Quick entry in site lists	Site management	Allows users to quickly create, delete, modify, and query sites.
		Qiankun Shield management	Allows users to create, delete, modify, and query Qiankun Shield devices.
	Messages	Threat event handling	Pushes emergency threat events to the app notification panel so that users can handle the events in a timely manner.
		Security service message	Pushes messages about new Huawei Qiankun security services to the app notification panel so that users can learn about these new services in a timely manner.

Level-1 Category	Level-2 Category	Item	Description
Personal center	Registration and login	Username login	Allows tenants to log in to the Huawei Qiankun app using usernames and passwords.
	Personal information	Profile picture modification	Allows tenants to modify profile pictures in the personal information.
		Tenant name modification	Allows tenants to modify their names.
		Email address linking or modification	Allows tenants to link email addresses to their accounts and modify the linked email addresses.
	Package management	-	Allows tenants to view package information of their accounts.
	Service tickets	Service ticket processing	1. Allows tenants to view historical service tickets of their accounts. 2. Allows tenants to send reminders, and close or review service tickets.
		Service ticket creation	Allows users to quickly create service tickets.
	Namecard	App sharing	1. Allows users to share the Huawei Qiankun app download link with one tap. 2. Allows users to share the app on WeChat Moments and to WeChat friends.
	Settings	About	1. Allows users to quickly view the latest privacy statement and customer agreement of Huawei Qiankun. 2. Supports one-tap query of the latest Huawei Qiankun app version.

2 Introduction to Licenses

- [2.1 Before You Start](#)
- [2.2 License-related Concepts](#)
- [2.3 License Control Items](#)

2.1 Before You Start

All services and solutions of Huawei Qiankun can be purchased offline, and some of them can be purchased online.

- **Online purchase:** Customers purchase services on the Huawei Cloud KooGallery on their own. Then, the services are automatically activated for customers to use.
- **Offline purchase:** Huawei product managers or channel partners purchase services for customers using the UniSTAR Smart Configuration Tool (SCT). Customers need to activate the services on the Huawei Qiankun platform based on license information, such as license entitlement IDs.

This document mainly describes the license information involved in offline purchase scenarios.

2.2 License-related Concepts

- **License:** A license is an agreement reached between the supplier and customer, authorizing the scope and period of using the purchased product (software in this document). The license enables you to obtain the services committed by the supplier. A license is composed of a license file and a license entitlement certificate.
- **License entitlement certificate**
A license entitlement certificate is also called a license certificate. It records license-related information such as the product name, entitlement ID (originally called LAC, which is short for license authorization code), customer name, and validity period. The certificate is used as credentials of owning a Huawei product license. A license entitlement certificate is delivered with

products in electronic format (PDF file), and can be downloaded from the Electronic Software Delivery Platform (ESDP) and then printed.

Only commercial licenses have license entitlement certificates.

- **ESDP**
ESDP is a system used by Huawei to generate and issue license keys based on purchase orders (POs) or application information and to manage license information.
ESDP website: <https://esdp.huawei.com/sdp2/#/home>
- **Equipment serial number (ESN)**
An ESN, also called device fingerprint, uniquely identifies a device and is key to authorizing a license to a specific device.
- **LAC**
An LAC, also called entitlement ID, is generated on the ESDP and used to authenticate users. On the ESDP website, you can enter license-related information, such as the LAC and ESN, to activate a license file. Huawei defines a LAC as an essential part of each license entitlement certificate.

2.3 License Control Items

Table 2-1 lists the license control items of the Border Protection and Response Service purchased offline.

Table 2-1 License control items

Service Name	License Control Item		Notes on Usage
Border Protection and Response Service NOTE A device must be purchased when you purchase a license of this service. License control items vary according to device models.	USG6530E/ USG6585E	License control items include: • Border Protection and Response (Standard Edition) • Threat Protection Database Upgrade Service • Border Protection Service – Automatic Threat Blocking	This service is available only after a corresponding license is activated on the cloud.

3 Device Alarm Handling

- 3.1 V300 AR Alarms
- 3.2 V500 Firewall Alarms
- 3.3 V200 LSW Alarms
- 3.4 WAC&AP Alarms
- 3.5 V600 Device Alarms

3.1 V300 AR Alarms

3.1.1 ALM-4287406190 A Device Is Reset

Description

ENTITYTRAP/3/BOARDRESET: OID [OID] The device has been reset.
(Index=[INTEGER], EntityPhysicalIndex=[INTEGER], PhysicalName="[OCTET]",
ResetInfo="[OCTET]")

The device restarts.

Attribute

Alarm ID	OID	Alarm Severity	Alarm Type
4287406190	1.3.6.1.4.1.2011.5.25.219.2.1.7	Minor	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
Index	Indicates the index.
EntityPhysicalIndex	Indicates a physical index.
EntPhysicalName	Indicates an entity name, which varies with the board type, such as SFU, LPU, and MPU.
ResetInfo	Indicates device restart information, including the restart reason and restart time.

Impact on the System

Service functions may be affected.

Possible Causes

- Cause 1: The restart command is manually executed, and the device has been restarted normally.
- Cause 2: The device has been restarted unexpectedly.

Procedure

- Run the **display reset-reason** command to check device restart information.
 - If the information indicates a normal restart such as **Reset by user command**, the device has been restarted normally, and no action is required.
 - If the information contains **exception**, the device has been restarted unexpectedly. You need to collect the information and then contact technical support personnel.

Clearing

The alarm needs to be cleared manually.

3.1.2 ALM-4287373328 A Board Is Removed

Description

ENTITYTRAP/4/BOARDREMOVE: OID [OID] Card has been removed.
(Index=[INTEGER], EntityPhysicalIndex=[INTEGER], PhysicalName="[OCTET]", EntityTrapEntType= [INTEGER], EntityTrapFaultID=[INTEGER])

A board was removed.

Attribute

Alarm ID	OID	Alarm Severity	Alarm Type
4287373328	1.3.6.1.4.1.2011.5.25.219.2.2.1	Major	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
Index	Indicates the index.
EntityPhysicalIndex	Indicates the physical entity index.
EntPhysicalName	Indicates the physical entity name.
EntityTrapEntType	Indicates the type of the physical entity, such as mpu(1) and lpu(2).
EntityTrapFaultID	Indicates the error code.

Impact on the System

All services on the board are interrupted.

Possible Causes

A board was removed.

Procedure

- Step 1** Check whether the board was removed manually.
- If so, no action is required.
 - If not, go to step 2.
- Step 2** Insert the corresponding board. After the board is started, run the **display device** command to check whether the board in the corresponding slot is registered successfully.
- If not, go to step 3.
 - If so, go to step 4.
- Step 3** Collect alarm information and configuration information, and then contact technical support personnel.
- Step 4** End.
- End

Clearing

The alarm needs to be cleared manually.

3.1.3 ALM-4287373329 A Board Is Inserted

Description

ENTITYTRAP/4/BOARDRINSERT: OID [OID] Board has been inserted.
(Index=[INTEGER], EntityPhysicalIndex=[INTEGER], PhysicalName="[OCTET]",
EntityTrapEntType= [INTEGER], EntityTrapFaultID=[INTEGER])

A board was inserted.

Attribute

Alarm ID	OID	Alarm Severity	Alarm Type
4287373329	1.3.6.1.4.1.201.1.5.25.219.2.2.2	Minor	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
Index	Indicates the index.
EntityPhysicalIndex	Indicates the physical entity index.
EntPhysicalName	Indicates the physical entity name.
EntityTrapEntType	Indicates the type of the entity type, such as mpu(1) and lpu(2).
EntityTrapFaultID	Indicates the error code.

Impact on the System

Services are not affected.

Possible Causes

A board was inserted.

Procedure

This alarm is informational only, and no action is required.

Clearing

The alarm needs to be cleared manually.

3.1.4 ALM-4287373322 Hardware fault

3.1.4.1 ALM-4287373322 Hardware fault 132103

Description

ENTITYTRAP/2/BOARDFAIL: OID [OID] Board become failure for some reason.
(Index=[INTEGER], EntityPhysicalIndex=[INTEGER], PhysicalName="[OCTET]",
EntityTrapEntType=[INTEGER], EntityTrapFaultID=132103)

Some functions on the board are invalid.

Attribute

Alarm ID	Alarm Severity	Alarm Type
4287373322	Critical	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
Index	Indicates the entity index.
EntityPhysicalIndex	Indicates the physical entity index.
EntPhysicalName	Indicates the name of the physical entity.
EntityTrapEntType	Indicates the type of the physical entity, such as mpu(1), and lpu(2).
EntityTrapFaultID	Indicates the error code.

Impact on the System

The board is unavailable or some services are interrupted.

Possible Causes

The battery of the main control board was faulty.

Procedure

Step 1 Check whether the faulty board is registered successfully and services are running properly.

Run the **display device** command to check whether the faulty board is registered successfully, and run the **display interface counters** command to view the statistics on received and sent packets. According to the statistics, check whether services are running properly.

- If the faulty board is registered successfully and services are running properly, no action is required.
- If the faulty board is unregistered or services are not running properly, go to step 2.

Step 2 If the faulty board is a main control board, run the **reboot** command to reboot the device. If the faulty board is an interface board, run the **reset slot** command to reset the faulty interface board. Then check whether the device is working properly.

- If the board can be registered successfully and services are running properly, no action is required.
- If the board cannot be registered or services cannot run properly, the board hardware is faulty. Replace this board.
- If the fault persists, go to step 3.

Step 3 Collect alarm information and configuration information, and then contact technical support personnel.

----End

Related Information

None

3.1.4.2 ALM-4287373322 Hardware fault 132105

Description

ENTITYTRAP/2/BOARDFAIL: OID [OID] Board become failure for some reason. (Index=[INTEGER], EntityPhysicalIndex=[INTEGER], PhysicalName="[OCTET]", EntityTrapEntType=[INTEGER], EntityTrapFaultID=132105)

Some functions on the board are invalid.

Attribute

Alarm ID	Alarm Severity	Alarm Type
4287373322	Critical	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
Index	Indicates the entity index.
EntityPhysicalIndex	Indicates the physical entity index.
EntPhysicalName	Indicates the name of the physical entity.
EntityTrapEntType	Indicates the type of the physical entity, such as mpu(1), and lpu(2).
EntityTrapFaultID	Indicates the error code.

Impact on the System

The board is unavailable or some services are interrupted.

Possible Causes

The board was faulty.

Procedure

Step 1 Check whether the faulty board is registered successfully and services are running properly.

Run the **display device** command to check whether the faulty board is registered successfully, and run the **display interface counters** command to view the statistics on received and sent packets. According to the statistics, check whether services are running properly.

- If the faulty board is registered successfully and services are running properly, no action is required.
- If the faulty board is unregistered or services are not running properly, go to step 2.

Step 2 If the faulty board is a main control board, run the **reboot** command to reboot the device. If the faulty board is an interface board, run the **reset slot** command to reset the faulty interface board. Then check whether the device is working properly.

- If the board can be registered successfully and services are running properly, no action is required.
- If the board cannot be registered or services cannot run properly, the board hardware is faulty. Replace this board.
- If the fault persists, go to step 3.

Step 3 Collect alarm information and configuration information, and then contact technical support personnel.

----End

Related Information

None

3.1.4.3 ALM-4287373322 Hardware fault 132106

Description

ENTITYTRAP/2/BOARDFAIL: OID [oid] Board become failure for some reason. (Index=[INTEGER], EntityPhysicalIndex=[INTEGER], PhysicalName="[OCTET]", EntityTrapEntType=[INTEGER], EntityTrapFaultID=132106)

Some functions on the board are invalid.

Attribute

Alarm ID	Alarm Severity	Alarm Type
4287373322	Critical	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
Index	Indicates the entity index.
EntityPhysicalIndex	Indicates the physical entity index.
EntPhysicalName	Indicates the name of the physical entity.
EntityTrapEntType	Indicates the type of the physical entity.
EntityTrapFaultID	Indicates the error code.

Impact on the System

The board is unavailable or some services are interrupted.

Possible Causes

The flash memory of the board was faulty.

Procedure

Step 1 Check whether the faulty board is registered successfully and services are running properly.

Run the **display device** command to check whether the faulty board is registered successfully, and run the **display interface counters** command to view the statistics on received and sent packets. According to the statistics, check whether services are running properly.

- If the faulty board is registered successfully and services are running properly, no action is required.
- If the faulty board is unregistered or services are not running properly, go to step 2.

Step 2 If the faulty board is a main control board, run the **reboot** command to reboot the device. If the faulty board is an interface board, run the **reset slot** command to reset the faulty interface board. Then check whether the device is working properly.

- If the board can be registered successfully and services are running properly, no action is required.
- If the board cannot be registered or services cannot run properly, the board hardware is faulty. Replace this board.
- If the fault persists, go to step 3.

Step 3 Collect alarm information and configuration information, and then contact technical support personnel.

----End

Related Information

None

3.1.4.4 ALM-4287373322 Hardware fault 132121

Description

ENTITYTRAP/2/BOARDFAIL: OID [OID] Board become failure for some reason. (Index=[INTEGER], EntityPhysicalIndex=[INTEGER], PhysicalName="[OCTET]", EntityTrapEntType=[INTEGER], EntityTrapFaultID=132121)

Some functions on the board are invalid.

Attribute

Alarm ID	Alarm Severity	Alarm Type
4287373322	Critical	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
Index	Indicates the entity index.
EntityPhysicalIndex	Indicates the physical entity index.
EntPhysicalName	Indicates the name of the physical entity.
EntityTrapEntType	Indicates the type of the physical entity, such as mpu(1), and lpu(2).
EntityTrapFaultID	Indicates the error code.

Impact on the System

The board is unavailable or some services are interrupted.

Possible Causes

The USB controller on the board was faulty.

Procedure

Step 1 Check whether the faulty board is registered successfully and services are running properly.

Run the **display device** command to check whether the faulty board is registered successfully, and run the **display interface counters** command to view the statistics on received and sent packets. According to the statistics, check whether services are running properly.

- If the faulty board is registered successfully and services are running properly, no action is required.
- If the faulty board is unregistered or services are not running properly, go to step 2.

Step 2 If the faulty board is a main control board, run the **reboot** command to reboot the device. If the faulty board is an interface board, run the **reset slot** command to reset the faulty interface board. Then check whether the device is working properly.

- If the board can be registered successfully and services are running properly, no action is required.
- If the board cannot be registered or services cannot run properly, the board hardware is faulty. Replace this board.
- If the fault persists, go to step 3.

Step 3 Collect alarm information and configuration information, and then contact technical support personnel.

----End

Related Information

None

3.1.4.5 ALM-4287373322 Hardware fault 132128

Description

ENTITYTRAP/2/BOARDFAIL: OID [OID] Board become failure for some reason. (Index=[INTEGER], EntityPhysicalIndex=[INTEGER], PhysicalName="[OCTET]", EntityTrapEntType=[INTEGER], EntityTrapFaultID=132128)

Some functions on the board are invalid.

Attribute

Alarm ID	Alarm Severity	Alarm Type
4287373322	Critical	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
Index	Indicates the entity index.
EntityPhysicalIndex	Indicates the physical entity index.
EntPhysicalName	Indicates the name of the physical entity.
EntityTrapEntType	Indicates the type of the physical entity, such as mpu(1), and lpu(2).
EntityTrapFaultID	Indicates the error code.

Impact on the System

The board is unavailable or some services are interrupted.

Possible Causes

The Phase-Locked Loop (PLL) was faulty.

Procedure

Step 1 Check whether the faulty board is registered successfully and services are running properly.

Run the **display device** command to check whether the faulty board is registered successfully, and run the **display interface counters** command to view the statistics on received and sent packets. According to the statistics, check whether services are running properly.

- If the faulty board is registered successfully and services are running properly, no action is required.
- If the faulty board is unregistered or services are not running properly, go to step 2.

Step 2 If the faulty board is a main control board, run the **reboot** command to reboot the device. If the faulty board is an interface board, run the **reset slot** command to reset the faulty interface board. Then check whether the device is working properly.

- If the board can be registered successfully and services are running properly, no action is required.
- If the board cannot be registered or services cannot run properly, the board hardware is faulty. Replace this board.
- If the fault persists, go to step 3.

Step 3 Collect alarm information and configuration information, and then contact technical support personnel.

----End

Related Information

None

3.1.4.6 ALM-4287373322 Hardware fault 132131

Description

ENTITYTRAP/2/BOARDFAIL: OID [OID] Board become failure for some reason. (Index=[INTEGER], EntityPhysicalIndex=[INTEGER], PhysicalName="[OCTET]", EntityTrapEntType=[INTEGER], EntityTrapFaultID=132131)

Some functions on the board are invalid.

Attribute

Alarm ID	Alarm Severity	Alarm Type
4287373322	Critical	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
Index	Indicates the entity index.
EntityPhysicalIndex	Indicates the physical entity index.
EntPhysicalName	Indicates the name of the physical entity.
EntityTrapEntType	Indicates the type of the physical entity, such as mpu(1), and lpu(2).
EntityTrapFaultID	Indicates the error code.

Impact on the System

The board is unavailable or some services are interrupted.

Possible Causes

The board was faulty.

Procedure

Step 1 Check whether the faulty board is registered successfully and services are running properly.

Run the **display device** command to check whether the faulty board is registered successfully, and run the **display interface counters** command to view the statistics on received and sent packets. According to the statistics, check whether services are running properly.

- If the faulty board is registered successfully and services are running properly, no action is required.
- If the faulty board is unregistered or services are not running properly, go to step 2.

Step 2 If the faulty board is a main control board, run the **reboot** command to reboot the device. If the faulty board is an interface board, run the **reset slot** command to reset the faulty interface board. Then check whether the device is working properly.

- If the board can be registered successfully and services are running properly, no action is required.
- If the board cannot be registered or services cannot run properly, the board hardware is faulty. Replace this board.
- If the fault persists, go to step 3.

Step 3 Collect alarm information and configuration information, and then contact technical support personnel.

----End

Related Information

None

3.1.4.7 ALM-4287373322 Hardware fault 132137

Description

ENTITYTRAP/2/BOARDFAIL: OID [OID] Board become failure for some reason. (Index=[INTEGER], EntityPhysicalIndex=[INTEGER], PhysicalName="[OCTET]", EntityTrapEntType=[INTEGER], EntityTrapFaultID=132137)

Some functions on the board are invalid.

Attribute

Alarm ID	Alarm Severity	Alarm Type
4287373322	Critical	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
Index	Indicates the entity index.
EntityPhysicalIndex	Indicates the physical entity index.
EntPhysicalName	Indicates the name of the physical entity.
EntityTrapEntType	Indicates the type of the physical entity, such as mpu(1), and lpu(2).
EntityTrapFaultID	Indicates the error code.

Impact on the System

The board is unavailable or some services are interrupted.

Possible Causes

The chip of the board was faulty.

Procedure

Step 1 Check whether the faulty board is registered successfully and services are running properly.

Run the **display device** command to check whether the faulty board is registered successfully, and run the **display interface counters** command to view the statistics on received and sent packets. According to the statistics, check whether services are running properly.

- If the faulty board is registered successfully and services are running properly, no action is required.
- If the faulty board is unregistered or services are not running properly, go to step 2.

Step 2 If the faulty board is a main control board, run the **reboot** command to reboot the device. If the faulty board is an interface board, run the **reset slot** command to reset the faulty interface board. Then check whether the device is working properly.

- If the board can be registered successfully and services are running properly, no action is required.
- If the board cannot be registered or services cannot run properly, the board hardware is faulty. Replace this board.
- If the fault persists, go to step 3.

Step 3 Collect alarm information and configuration information, and then contact technical support personnel.

----End

Related Information

None

3.1.4.8 ALM-4287373322 Hardware fault 132146

Description

ENTITYTRAP/2/BOARDFAIL: OID [OID] Board become failure for some reason. (Index=[INTEGER], EntityPhysicalIndex=[INTEGER], PhysicalName="[OCTET]", EntityTrapEntType=[INTEGER], EntityTrapFaultID=132146)

Some functions on the board are invalid.

Attribute

Alarm ID	Alarm Severity	Alarm Type
4287373322	Critical	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
Index	Indicates the entity index.
EntityPhysicalIndex	Indicates the physical entity index.
EntPhysicalName	Indicates the name of the physical entity.
EntityTrapEntType	Indicates the type of the physical entity, such as mpu(1), and lpu(2).
EntityTrapFaultID	Indicates the error code.

Impact on the System

The Ethernet port cannot provide PoE power for PDs.

Possible Causes

The PoE chip on the board is faulty.

Procedure

Step 1 Check whether the faulty board is registered successfully and services are running properly.

Run the **display device** command to check whether the faulty board is registered successfully, and run the **display interface counters** command to view the statistics on received and sent packets. According to the statistics, check whether services are running properly.

- If the faulty board is registered successfully and services are running properly, no action is required.
- If the faulty board is unregistered or services are not running properly, go to step 2.

Step 2 If the faulty board is a main control board, run the **reboot** command to reboot the device. If the faulty board is an interface board, run the **reset slot** command to reset the faulty interface board. Then check whether the device is working properly.

- If the board can be registered successfully and services are running properly, no action is required.
- If the board cannot be registered or services cannot run properly, the board hardware is faulty. Replace this board.
- If the fault persists, go to step 3.

Step 3 Collect alarm information and configuration information, and then contact technical support personnel.

----End

Related Information

None

3.1.4.9 ALM-4287373322 Hardware fault 132154

Description

ENTITYTRAP/2/BOARDFAIL: OID [OID] Board become failure for some reason. (Index=[INTEGER], EntityPhysicalIndex=[INTEGER], PhysicalName="[OCTET]", EntityTrapEntType=[INTEGER], EntityTrapFaultID=132154)

Some functions on the board are invalid.

Attribute

Alarm ID	Alarm Severity	Alarm Type
4287373322	Critical	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
Index	Indicates the entity index.
EntityPhysicalIndex	Indicates the physical entity index.
EntPhysicalName	Indicates the name of the physical entity.
EntityTrapEntType	Indicates the type of the physical entity, such as mpu(1), and lpu(2).
EntityTrapFaultID	Indicates the error code.

Impact on the System

The voice interface feed was abnormal and calls cannot be connected.

Possible Causes

The voice interface feed was abnormal.

Procedure

Step 1 Check whether the faulty board is registered successfully and services are running properly.

Run the **display device** command to check whether the faulty board is registered successfully, and run the **display interface counters** command to view the statistics on received and sent packets. According to the statistics, check whether services are running properly.

- If the faulty board is registered successfully and services are running properly, no action is required.
- If the faulty board is unregistered or services are not running properly, go to step 2.

Step 2 If the faulty board is a main control board, run the **reboot** command to reboot the device. If the faulty board is an interface board, run the **reset slot** command to reset the faulty interface board. Then check whether the device is working properly.

- If the board can be registered successfully and services are running properly, no action is required.
- If the board cannot be registered or services cannot run properly, the board hardware is faulty. Replace this board.
- If the fault persists, go to step 3.

Step 3 Collect alarm information and configuration information, and then contact technical support personnel.

----End

Related Information

None

3.1.5 ALM-4287373416 Insufficient Storage Space

Description

ENTITYTRAP/3/STORAGEINSUFFICIENT:OID [OID] Storage utilization exceeded the alarm threshold. (Index=[INTEGER], PhysicalName="[OCTET]", StorageName="[OCTET]", ThresholdValue=[INTEGER](KB), CurrentValue=[INTEGER](KB))

The storage space was insufficient.

Attribute

Alarm ID	OID	Alarm Severity	Alarm Type
4287373416	1.3.6.1.4.1.201.1.5.25.219.2.2.34	Major	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
Index	Indicates a physical index.
PhysicalName	Indicates an entity name.
StorageName	Indicates the storage device name.
ThresholdValue	Indicates the alarm threshold.
CurrentValue	Indicates the current value.

Impact on the System

Logs or other data cannot be saved.

Possible Causes

Too many files (such as logs) were stored or generated on the device.

Procedure

- Step 1

Run the **delete** *filename* command in the user view to delete the specified file in the storage device. *filename* specifies the name of a file to be deleted.
- Step 2

Run the **reset recycle-bin** command to clear a file from the recycle bin. Clean up the disk space.

NOTICE

If you delete a file by using the **delete/unreserved** *filename* command in the user view, the file cannot be restored.

----End

Clearing

After the fault is rectified, the system clears this alarm, removing the need to manually clear it. This alarm will not be displayed on the **Current Alarms** page.

3.1.6 ALM-4287373398 System Rollback

Description

NTITYTRAP/1/SYSTEMROLL:OID [oid] System rollback.(Reason="[OCTET]",Version="[OCTET]",FileName="[OCTET]")

Rollback occurs on the system.

AttributeAfter the root directory is formatted

Alarm ID	OID	Alarm Severity	Alarm Type
4287373398	1.3.6.1.4. 1.2011.5. 25.219.2. 11.3	Critical	Processing error alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
Reason	Indicates the error code.
Version	Indicates the version before the rollback.
FileName	Indicates the file name.

Impact on the System

The system software supports only the service features of the current version after the startup succeeds.

The system does not support clear alarms. You need to manually clear this alarm.

Possible Causes

- If the specified startup software fails when you upgrade the system software or restart the device, the system will use the software that works last time. This alarm is generated when the startup succeeds, indicating that a version rollback occurs. If the startup fails, the system will use the specified backup software. This alarm is generated when the startup succeeds, indicating that a version rollback occurs.
- If a fault occurs in the flash memory, the system starts from the backup partition of the flash memory. You need to rectify the fault.

Procedure

Step 1 If the rollback reason is System software rollback, perform the following operations:

1. Run the **dir** command to check the file system.
 - If the storage medium is unavailable, the storage medium is corrupted. Go to step 2.
 - If the software that fails to start the system is in the file system, check the file size. If the file size is not in the allowed range, the system software is invalid. Go to step 3.
 - If the storage medium is available and the file size is within the allowed range, system software is faulty and cannot start the system. Go to step 4.
2. Check the storage medium saved in the system software.
 - If the storage medium is an SD card or a USB disk, replace it and restart the upgrade. If the upgrade fails, go to step 4.
 - If the storage medium is flash, record the device type and number and collect alarm information and configuration information, and then contact technical support personnel.
3. Delete the invalid file and upload a complete file. Perform the upgrade. If the upgrade fails, go to step 4.
4. Collect operation results and collect alarm information and configuration information, and then contact technical support personnel.

Step 2 If the rollback reason is Backup flash space rollback, the system starts from the backup partition of the flash memory. You need to perform the following operations to rectify the fault:

1. Run the **display startup** command in the user view to check information about the current startup system software and configuration file. If the command output shows that the storage path of the system software or configuration file is backup:/, it indicates that the device starts from the secondary flash partition.
2. Run the **format flash:** command in the user view to format the root directory of the flash memory.

NOTE

After this command is executed, all files and directories in the specified storage medium will be cleared and cannot be restored. Therefore, use this command with caution.

3. After the root directory is formatted, run the **cd flash:** command to change the current working directory to flash. Then, upload the target system software and configuration file to the flash memory through SFTP.
4. After the files are uploaded, run the **startup system-software** *system-file* [**slave-board** | **all**] [**verify** | **signature** *sign-filename*] command to specify the system software used for the next startup.
5. Run the **startup saved-configuration** *configuration-file* [**slave-board** | **all**] command to specify the configuration file used for the next startup.
6. After the configurations are complete, check whether the alarm is displayed again. If the alarm persists, contact technical support personnel.

Step 3 If the rollback reason is "System software rollback after upgrade, the possible cause is that new version can't register iMaster NCE-Campus": Collect alarm information and configuration information, and then contact technical support personnel.

 NOTE

This cause is supported in V300R022C00SPC100 and later versions.

----End

Clearing

The alarm needs to be cleared manually.

3.1.7 ALM-4287373404 CPU Utilization Exceeds the Threshold

Description

ENTITYTRAP/2/CPUUSAGERISING: OID [OID] CPU utilization exceeded the pre-alarm threshold. (Index=[INTEGER], HwEntityPhysicalIndex=[INTEGER], PhysicalName="[OCTET]", EntityThresholdType=[INTEGER], EntityThresholdWarning=[INTEGER], EntityThresholdCurrent=[INTEGER], EntityTrapFaultID=[INTEGER])

The CPU is overloaded.

Attribute

Alarm ID	OID	Alarm Severity	Alarm Type
4287373404	1.3.6.1.4.1.201.1.5.25.219.2.1.4.1	Major	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
Index	Indicates the entity index.
HwEntityPhysicalIndex	Indicates the physical entity index.
PhysicalName	Indicates the physical entity name.
EntityThresholdType	Indicates the threshold type.
EntityThresholdWarning	Indicates the alarm threshold.
EntityThresholdCurrent	Indicates the current CPU usage.
EntityTrapFaultID	Indicates the error code.

Impact on the System

The system responds slowly.

Possible Causes

Operations are frequently performed on services.

Procedure

View the log **CPUP/4/CPU_USAGE_HIGH** to check the CPU usage of each task and contact technical support personnel.

Clearing

After the fault is rectified, the system clears this alarm, removing the need to manually clear it. This alarm will not be displayed on the **Current Alarms** page.

3.1.8 ALM-4287373406 Memory Utilization Exceeds the Threshold

Description

ENTITYTRAP/2/MEMORYUSAGERISING: OID [OID] MEMORY utilization exceeded the pre-alarm threshold. (Index=[INTEGER], HwEntityPhysicalIndex=[INTEGER], PhysicalName="[OCTET]", EntityThresholdType=[INTEGER], EntityThresholdWarning=[INTEGER], EntityThresholdCurrent=[INTEGER], EntityTrapFaultID=[INTEGER])

The memory usage is too high.

Attribute

Alarm ID	OID	Alarm Severity	Alarm Type
4287373406	1.3.6.1.4.1.201.1.5.25.219.2.1.5.1	Major	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
Index	Indicates the entity index.
HwEntityPhysicalIndex	Indicates the physical entity index.
PhysicalName	Indicates the physical entity name.
EntityThresholdType	Indicates the threshold type.
EntityThresholdWarning	Indicates the alarm threshold.
EntityThresholdCurrent	Indicates the current memory usage.
EntityTrapFaultID	Indicates the error code.

Impact on the System

Services are affected. The system will restart after generating this alarm.

Possible Causes

Too many services are configured.

Procedure

Run the **display current-configuration** command to check service configurations and contact technical support personnel.

Clearing

After the fault is rectified, the system clears this alarm, removing the need to manually clear it. This alarm will not be displayed on the **Current Alarms** page.

3.1.9 ALM-4287373399 Storage Media Remove

Description

ENTITYTRAP/4/STORAGEREMOVE:OID [OID] Storage remove.
(Index=[INT],PhysicalName="[OCTET]",StorageName="[OCTET]")

This alarm is generated when a storage card is removed.

Attribute

Alarm ID	OID	Alarm Severity	Alarm Type
4287373399	1.3.6.1.4.1.201.1.5.25.219.2.1.6.1	Minor	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
Index	Indicates the physical entity index.
PhysicalName	Indicates the name of an entity.
StorageName	Indicates the storage device name.

Impact on the System

If the **is pulled out** alarm is displayed when the storage device is installed, the configuration file and log file may be lost.

Possible Causes

The storage device is pulled out.

Procedure

Check whether the storage device is removed. If not, contact technical support personnel.

Clearing

The alarm needs to be cleared manually.

3.1.10 ALM-4287373400 Storage Media Is Inserted

Description

ENTITYTRAP/4/STORAGEINSERT:OID [OID] Storage insert.
(Index=[INT],PhysicalName="[OCTET]",StorageName="[OCTET]")

This alarm is generated when a storage card is inserted.

Attribute

Alarm ID	OID	Alarm Severity	Alarm Type
4287373400	1.3.6.1.4.1.201.1.5.25.219.2.1.6.2	Minor	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
Index	Indicates the physical entity index.
PhysicalName	Indicates the name of an entity.
StorageName	Indicates the storage device name.

Impact on the System

None

Possible Causes

A storage device is inserted.

Procedure

Check whether the storage device is inserted. If not, contact technical support personnel.

Clearing

The alarm needs to be cleared manually.

3.1.11 ALM-4285734913 IPSec Tunnel Is Deleted

Description

IPSEC/4/IPSECTUNNELSTOP: OID [OID] The IPSec tunnel is deleted.
(Ifindex=[Ifindex], SeqNum=[SeqNum],TunnelIndex=[TunnelIndex],
RuleNum=[RuleNum], DstIP=[DstIP], InsideIP=[InsideIP],
RemotePort=[RemotePort], CpuID=[CpuID], SrcIP=[SrcIP], FlowInfo=[FlowInfo],
OfflineReason=[offlinereason], VsysName=[vsys-name],
InterfaceName=[InterfaceName], SlotID=[SlotID])

An IPSec tunnel is deleted.

Attribute

Alarm ID	Alarm Severity	Alarm Type
4285734913	Major	Communication alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
Ifindex	Indicates the interface index.
SeqNum	Indicates the policy number.
TunnelIndex	Indicates the tunnel index.
RuleNum	Indicates the rule number.
DstIP	Indicates the IP address of the peer end of the IPSec tunnel.
InsideIP	Indicates the intranet IP address of the peer end of the tunnel.

Name	Meaning
RemotePort	Indicates the port number of the peer end of the IPsec tunnel.
CpuID	Indicates the CPU number.
SrcIP	Indicates the IP address of the local end of the IPsec tunnel.
FlowInfo	Indicates the data flow information of the IPsec tunnel, including the source address, destination address, ACL port number, ACL protocol number, and DSCP.
offlinereason	Indicates the reason why the IPsec tunnel was deleted.
vsys-name	Indicates the name of the virtual system to which the IPsec policy belongs. NOTE The device does not support this parameter.
InterfaceName	Indicates the interface name.
SlotID	Indicates the slot number. NOTE The device does not support this parameter.

Impact on the System

An IPsec tunnel has been deleted.

Possible Causes

An IPsec tunnel has been deleted due to the following causes:

- dpd timeout: Dead peer detection (DPD) times out.
- config modify or manual offline: An SA is deleted due to configuration modification or an SA is manually deleted.
- modecfg address soft expiry: The IP address lease applied by the remote end from the server expires.
- re-auth timeout: An SA is deleted due to reauthentication timeout.
- aaa cut user: The AAA module disconnects users.
- kick old sa with same flow: The old SA is deleted for the same incoming flow.
- spi conflict: An SPI conflict occurs.
- phase1 sa replace: The new IKE SA replaces the old IKE SA.

- phase2 sa replace: The new IPsec SA replaces the old IPsec SA.
- disconnect track nqa/bfd/vrrp: The IPsec tunnel is torn down based on the NQA test instance, NQA group, VRRP, BFD session, or BFD group status.
- receive invalid spi notify: The device receives an invalid SPI notification.
- dns resolution status change: DNS resolution status changes.
- ikev1 phase1-phase2 sa dependent offline: The device deletes the associated IPsec SA when deleting an IKEv1 SA.
- exchange timeout: Packet interaction timeout.

Procedure

- Cause: dpd timeout
Log in to the iMaster NCE-Campus as a tenant administrator. Choose **Maintenance > Diagnosis > Ping** from the main menu. In the **Results** area, check the link status of the corresponding device.
 - If the link status is normal, no operation is required.
 - If not, check whether the link and network configurations are correct.
- Cause: config modify or manual offline
 - a. Check whether the tunnel is deleted manually or whether the SA is reset. If so, no operation is required.
 - b. Log in to the iMaster NCE-Campus as a tenant administrator. Choose **Maintenance > Provisioning Result > Site Configuration Status** from the main menu.
 - c. On the **Configuration Result** tab page, click  next to a device, click **IPsec** on the **Feature List** tab page, and click **For Details** to view the IPsec status of the corresponding device.
 - If the link status is normal, no operation is required.
 - If not, modify the IPsec configuration.
- Cause: receive invalid spi notify
If this fault occurs frequently, check whether the remote device status or configurations are abnormal.
 - a. Check the device status.
Log in to the iMaster NCE-Campus as a tenant administrator. Choose **Design > Site Design > Device Management** from the main menu, check the status of the corresponding device.
 - If the status is normal, no operation is required.
 - If not, click the device name to go to the details page and locate the fault.
 - b. Check the status of IPsec and NHRP on the peer device.
 - i. Run the **display nhrp peer** command to check the NHRP peer table to locate the fault.
 - ii. Run the **display ike sa** command to check the SA status. If no IKE SA is established, the IPsec tunnel fails to be set up.

- Cause: dns resolution status change
 - a. Ensure that the link between the device and DNS server is normal.
 - b. Ensure that the DNS server is working properly.
 - c. Ensure that the domain name configured using the **remote-address host-name** command is correct.

- Cause: ikev1 phase1-phase2 sa dependent offline

This symptom is normal and no operation is required if the devices at two ends can renegotiate the IKE SA and IPSec SA. Otherwise, Log in to the iMaster NCE-Campus as a tenant administrator. Choose **Maintenance > Provisioning Result > Site Configuration Status** from the main menu.

On the **Configuration Result** tab page, click  next to a device, click **IPSec** on the **Feature List** tab page, and click **For Details** to view the IPSec status of the corresponding device.

- If the link status is normal, no operation is required.
- If not, modify the IPSec configuration.

- Cause: exchange timeout

Log in to the iMaster NCE-Campus as a tenant administrator. Choose **Maintenance > Diagnosis > Ping** from the main menu. In the **Results** area, check the link status of the corresponding device.

- If the link status is normal, no operation is required.
- If not, check whether the link and network configurations are correct.

- Cause: kick old sa with same flow

Run the **ipsec remote traffic-identical accept** command to allow branch or other users to quickly access the headquarters network.

- Cause: aaa cut user, disconnect track nqa/bfd/vrrp, modecfg address soft expiry, re-auth timeout, phase1 sa replace, phase2 sa replace, spi conflict
This symptom is normal and no operation is required.

Clearing

The alarm needs to be cleared manually.

3.1.12 ALM-4286128130 The Status of Hub NHRP Is Up

Description

NHRP/4/NHRPHUBUP: OID [oid] NHRP hub is up. (Interface=[interface-name], protocol-address=[protocol-address], mask=[mask], next-hop=[next-hop-address], nbma-address=[nbma-address], type=[peer-type])

The status of the Hub's NHRP mapping entry is Up.

Attribute

Alarm ID	Alarm Severity	Alarm Type
4286128130	Warning	Communication alarm

Parameters

Name	Meaning
<i>oid</i>	Indicates the MIB object ID of the alarm.
<i>interface-name</i>	Indicates the tunnel interface name specified in the NHRP mapping entry.
<i>protocol-address</i>	Indicates the protocol address in the NHRP mapping entry.
<i>mask</i>	Indicates the mask of the protocol address.
<i>next-hop-address</i>	Indicates the next-hop IP address to the protocol address.
<i>nbma-address</i>	Indicates the public network address in the NHRP mapping entry.
<i>peer-type</i>	Indicates the type of the NHRP mapping entry. The value can be: • hub: The NHRP mapping entry is generated during NHRP registration. • static: The NHRP mapping entry is configured by the administrator. • dynamic: The NHRP mapping entry is dynamically generated by the device.

Impact on the System

Services are not affected.

Possible Causes

After an NHRP mapping entry is configured on the Spoke, the Spoke sends a registration request to the Hub. After receiving a registration reply from the Hub, the Spoke records that the status of the Hub's NHRP mapping entry is Up.

Procedure

This log message is informational only, and no action is required.

Clearing

The alarm needs to be cleared manually.

3.1.13 ALM-4286128131 The Status of Hub NHRP Is Down

Description

NHRP/4/NHRPHUBDOWN: OID [OID] NHRP hub is down. (Interface=[interface-name], protocol-address=[protocol-address], mask=[mask], next-hop=[next-hop-address], nbma-address=[nbma-address])

The status of the Hub's NHRP mapping entry is Down.

Attribute

Alarm ID	OID	Alarm Severity	Alarm Type
4286128131	1.3.6.1.4.1.201.1.6.122.73.0.2.4	Major	Communication alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
interface-name	Indicates the tunnel interface name specified in the NHRP mapping entry.
protocol-address	Indicates the protocol address in the NHRP mapping entry.
mask	Indicates the mask of the protocol address.
next-hop-address	Indicates the next-hop IP address to the protocol address.
nbma-address	Indicates the public network address in the NHRP mapping entry.

Impact on the System

Services are not affected.

Possible Causes

Cause 1:

The tunnel interface goes down.

Cause 2:

The IPsec tunnel goes down.

Cause 3:

The APN status goes down.

Procedure

Step 1 Check whether the configuration is correct.

Run the **display interface brief** command to check the status of the tunnel interface.

- If the physical status of the interface is **Down**, check whether the link connected to the interface is normal. If not, rectify the fault.
- If the link protocol status of the interface is **Down**, rectify the fault according to the actual cause.

Step 2 Check whether the IPsec tunnel is deleted.

- If so, see [3.1.11 ALM-4285734913 IPsec Tunnel Is Deleted](#) to rectify the fault.
- If not, no operation is required.

Step 3 Check whether the status down of the Hub's NHRP mapping entry is caused by a normal operation.

Run the **display nhrp peer** command to check the NHRP peer table.

Step 4 If a misoperation is performed, contact technical support personnel.

----End

Clearing

After the certificate is deleted, the system clears this alarm, removing the need to manually clear it. This alarm will not be displayed on the **Current Alarms** page.

3.1.14 ALM-3488620545 The Status of the Link Is Down

Description

IFNET/1/IF_LINKDOWN: OID [OID] Interface [interface-index] turned into DOWN state.
(AdminStatus=[INTEGER],OperStatus=[INTEGER],InterfaceName=[OCTET],Description=[OCTET])

The status of the link protocol on the interface became Down.

Attribute

Alarm ID	OID	Alarm Severity	Alarm Type
3488620545	1.3.6.1.6.3.1.1.5.3	Critical	other

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
interface-index	Indicates the interface index.
AdminStatus	Indicates the admin status, which means whether the interface has been disabled. • 1: undo shutdown • 2: shutdown
OperStatus	Indicates the operating status, which means the link layer protocol status of the interface. • 1: Up • 2: Down
InterfaceName	Indicates the interface name.
Description	Indicates the interface description.

Impact on the System

The interface cannot forward packets normally.

Possible Causes

Cause 1:

The interface became Down and the link was disconnected.

Cause 2:

The VLANIF interface is deleted.

Procedure

Step 1 If the VLANIF interface is deleted, this alarm message is informational only. No action is required, go to step 7.

- Step 2** Run the **display this** command in the interface view to check whether interfaces on both ends are shut down.
- If so, go to step 3.
 - If not, go to step 4.
- Step 3** Run the **undo shutdown** command in the interface view to check whether the alarm is cleared.
- If so, go to step 7.
 - If not, go to step 4.
- Step 4** Check whether the cable and optical module are loosened or dropped.
- If so, go to step 6.
 - If not, go to step 5.
- Step 5** Connect the physical link correctly and then check whether the alarm is cleared.
- If so, go to step 7.
 - If not, go to step 6.
- Step 6** Collect alarm information and configuration information, and then contact technical support personnel.
- Step 7** End.
- End

Clearing

After the certificate is deleted, the system clears this alarm, removing the need to manually clear it. This alarm will not be displayed on the **Current Alarms** page.

3.1.15 ALM-4287373418 Battery fault

Description

BATTERY/4/BATTERY_TRAP(t):OID [OID] The battery status is abnormal.
(FaultReason="[octet string]")

The battery becomes faulty. Possible causes include battery aging and defect.

Attribute

Alarm ID	Alarm Severity	Alarm Type
4287373418	Warning	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
FaultReason	Indicates the reason for the abnormal battery status.

Impact on the System

After the DC is removed, the battery cannot provide power to the device normally.

Possible Causes

Cause 1:

The battery has aged, for example, it battery has been used for a long time and becomes unavailable.

Cause 2:

The battery has defects, for example, it is faulty before delivery or discharges fast.

Cause 3:

The battery is removed.

Procedure

Run the **display battery information** command in the diagnostic view to check the battery status. If the battery status displays defect, aging, or removal, replace this battery.

Related Information

None

3.1.16 ALM-4287373420 Battery low

Description

BATTERY/4/BATTERY_TRAP(t):OID [OID] Available power of the battery is low. (PowerLowReason="[octet string]")

The battery does not have sufficient power.

Attribute

Alarm ID	Alarm Severity	Alarm Type
4287373420	Warning	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
PowerLowReason	Indicates that the battery power is low and the remaining power supply time of the battery is less than 1 or 4 hours.

Impact on the System

The battery power is insufficient. If this battery is still used to provide power, the device may be powered off.

Possible Causes

The battery power is insufficient, and the remaining power supply time of the battery is less than 1 or 4 hours.

Procedure

Run the **display battery information** command in the diagnostic view to check the remaining power supply time of the battery. If the remaining power supply time is insufficient, connect the device to an external power supply.

Related Information

None

3.1.17 ALM-4287373386 The Temperature Is Not Within the Threshold

Description

ENTITYTRAP/1/ENTITYBRDTEMPALARM:OID [OID] Temperature rises over or falls below the warning alarm threshold.
(Index=[INTEGER1],EntryPhysicalIndex=[INTEGER2], PhysicalName="[OCTET]", EntityThresholdType=[INTEGER3],EntityThresholdValue=[INTEGER4],EntityThresholdCurrent=[INTEGER5], EntityTrapFaultID=[INTEGER6])

This alarm is generated when the temperature is not within the threshold. You can run the **display temperature** command to view the alarm threshold.

Attribute

Alarm ID	OID	Alarm Severity	Alarm Type
4287373386	1.3.6.1.4.1.201.1.5.25.219.2.10.13	Critical	environmentalAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
Index	Indicates the index of a temperature sensor.
EntryPhysicalIndex	Indicates the sub-index of an entity.
PhysicalName	Indicates the name of an entity.
EntityThresholdType 1: rise over 2: fall below	Indicates the alarm type.
EntityThresholdValue	Indicates the alarm threshold.
EntityThresholdCurrent	Indicates the current temperature.
EntityTrapFaultID	Indicates the cause ID of the alarm.

Impact on the System

The board overheats. If the temperature is higher than the fatal high temperature threshold, the board will be powered off, leading to service interruption.

Possible Causes

The fan is faulty, causing high temperature of the board.

Procedure

- Step 1** Run the **display temperature all** command to check the device temperature.
- Step 2** Run the **display fan** command to check the fan status and speed. Cool the device quickly. If a fan alarm is displayed at the same time, replace the fan.
- End

Clearing

After the certificate is deleted, the system clears this alarm, removing the need to manually clear it. This alarm will not be displayed on the **Current Alarms** page.

3.1.18 ALM-3491241985 The BGP Neighbor Is Changed

Description

BGP/2/BACKWARD:OID [OID] The BGP FSM moves from a higher numbered state to a lower numbered state. (BgpPeerRemoteAddr=[ipaddr], InstanceId=[gauge], Afi=[integer], Safi=[integer], PeerType=[integer], PeerRemoteAddr=[binary], InterfaceIndex=[integer], BgpPeerLastError=[octet], BgpPeerState=[integer], BgpPeerUnavaiReason=[gauge], InterfaceName=[octet])

Indicates that this trap was generated when the BGP state machine moved from a higher numbered state, namely, OpenConfirm or Established, to a lower numbered state.

Attribute

Alarm ID	OID	Alarm Severity	Alarm Type
3491241985	1.3.6.1.2.1.15.7.2	Major	Communication alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
BgpPeerRemoteAddr	Indicates the address of the peer.
InstanceId	Instance ID
Afi	Address family
Safi	Sub-address family
PeerType	Peer type
PeerRemoteAddr	Peer address

Name	Meaning
InterfaceIndex	Interface index
BgpPeerLastError	Indicates the error code of the BGP Notification when the neighbor relationship is disconnected for the last time. The value is expressed in the format of [ErrorCode][ErrorSubCode]. [ErrorCode] refers to the error code and [ErrorSubCode] refers to the error subcode. Take the integer 35 as an example, figure 3 is the error code and figure 5 is the error subcode. For detailed information about the error code, refer to BGP Error Code. If the value is 0, it indicates that no error occurs.

Name	Meaning
BgpPeerState	Indicates the status of the BGP peer. • 1 Idle: indicates that BGP denies any request of entering. This is the initiatory status of BGP. Upon receiving a Start event, BGP initiates a TCP connection to the remote BGP peer, starts the ConnectRetry Timer with the initial value, listens for a TCP connection initiated by the remote BGP peer, and changes its state to Connect. • 2 Connect: indicates that BGP performs other actions after the TCP connection is set up. – If the TCP connection succeeds, BGP stops the ConnectRetry Timer, sends an Open message to the remote peer, and changes its state to OpenSent. – If the TCP connection fails, BGP restarts the ConnectRetry Timer with the initial value, continues to listen for a TCP connection initiated by the remote peer, and changes its state to Active. – If the ConnectRetry Timer has expired before a TCP connection is established, BGP restarts the timer with the initial value, initiates a TCP connection to the remote BGP peer, and stays in the Connect state. • 3 Active: indicates that BGP tries to set up TCP connection. This is the intermediate status of BGP. – If the TCP connection succeeds, BGP stops the ConnectRetry Timer, sends an Open message to the remote peer, and changes its state to OpenSent. – If the ConnectRetry Timer has expired before a TCP connection is established, BGP restarts the timer with the initial value and changes its state to Connect. – If BGP initiates a TCP connection with an unknown IP address, the

Name	Meaning
	TCP connection fails. When this occurs, BGP restarts the ConnectRetry Timer with the initial value and stays in the Active state. ● 4 OpenSent: indicates that BGP has sent one Open message to its peer and waits for the other Open message from the peer. – If there are no errors in the Open message received, BGP changes its state to OpenConfirm. – If there are errors in the Open message received, BGP sends a Notification message to the remote peer and changes its state to Idle. – If the TCP connection fails, BGP restarts the ConnectRetry Timer with the initial value, continues to listen for a TCP connection initiated by the remote peer, and changes its state to Active. ● 5 OpenConfirm: indicates that BGP waits for a Notification message or a Keepalive message. – If BGP receives a Notification message, or the TCP connection fails, BGP changes its state to Idle. – If BGP receives a Keepalive message, BGP changes its state to Established. ● 6 Established: indicates that BGP peers can exchange Update, Notification and Keepalive packets. – If BGP receives an Update or a Keepalive message, its state stays in Established. – If BGP receives a Notification message, BGP changes its state to Idle.

Name	Meaning
BgpPeerUnavaiReason	Cause for the peer disconnection • 1 Configuration lead peer down: The configuration causes the peer disconnection. • 2 Receive notification: Notification packets are received. • 3 Receive error packet: Error packets are received. • 4 Hold timer expire: The Hold timer expires. • 5 Remote peer not reachable: The remote peer is unreachable. • 6 Direct connect-interface down: The directly connected interface is Down. • 7 Route limit: The number of routes exceeds the upper limit.
InterfaceName	Interface name

Impact on the System

The BGP neighbor will be disconnected, and the BGP route received from the neighbor will be deleted. The packet forwarding based on the BGP route will fail.

Possible Causes

1. The BGP holdtimer timed out and did not receive the Keepalive packet.
2. BGP received incorrect BGP packets.
3. The BGP neighbor relationship was reset and the neighbor relationship was automatically interrupted.
4. BGP received Notification packets from the neighbor.

Procedure

- Step 1** Run the **display bgp peer ipv4-addresses log-info** command to check the Error field in the command output. You can view the Error Code and Sub Error Code in the received Notification in the form of [ErrorCode][ErrorSubCode].
- If the error code of the Notification is 1, it indicates that the BGP module receives the packet with incorrect headers. Then, go to step 23.
 - If the error code of the Notification is 2, it indicates that the BGP module receives the incorrect Open packet. Then, go to step 23.
 - If the error code of the Notification is 3, it indicates that the BGP module receives the incorrect Update packet. Then, go to step 23.

- If the error code of the Notification is 4, it indicates that till the Holdtimer times out, the BGP module does not receive the Keepalive packet. Then, go to step 4.
- If the error code of the Notification is 5, it indicates that the finite state machine of the BGP module is faulty. Then, go to step 23.
- If the error code of the Notification is 6, go to step 2.
- If the error code of the Notification is 4 and error subcode is 6, it indicates that the BGP peer device proactively tears down the connection.

Step 2 If the error code of the Notification is 6, it indicates that BGP automatically closes the connection. Then, you need to run the **display bgp peer ipv4-address log-info** command to view the Notification field and check whether the Notification is sent by the router that generates the alarm.

- If "Send Notification" is displayed, it indicates that the local router actively sends the Notification. Then, go to step 3.
- If "Receive Notification" is displayed, it indicates that the local router receives the Notification. Then, go to step 22.

Step 3 Search for the **reset bgp all** and **reset bgp ipv4-address** commands in the user logs to check whether BGP is reset on the local end; or search for the **peer ipv4-address enable** command to check whether the peer is enabled in other address families on the local, or parameters for the BGP connection are configured.

- If so, it indicates that incorrect configurations cause the alarm, and thus no action is required. Then, go to step 24.
- If not, go to step 23.

Step 4 If the error code is 4, it indicates that the BGP disconnection is caused by the timeout of the Holdtimer. Then, you need to check whether the address of the BGP neighbor can be pinged successfully.

- If so, go to step 21.
- If not, go to step 5.

Step 5 Run the **display ip routing-table** command to check whether the Destination/Mask field has the route to the peer address.

- If so, go to step 7.
- If not, go to step 8.

Step 6 Run the **display acl all** command to check whether the router is configured with the ACL that disables TCP port 179.

- If so, go to step 9.
- If not, go to step 10.

Step 7 Run the **display ip interface brief** command to check whether the values of Physical and Protocol fields of the outbound interface are Up.

- If so, go to step 23.
- If not, go to step 11.

Step 8 Check the origin of the route with the BGP peer address.

- If the route is originated from OSPF, go to step 12.
- If the route is originated from IS-IS, go to step 13.

- Else, go to step 23.
- Step 9** Delete the ACL that disables the TCP port 179, and check whether the alarm BGP_1.3.6.1.4.1.2011.5.25.177.1.3.9 hwBgpPeerEstablished appears later.
 - If so, go to step 24.
 - If not, go to step 10.
- Step 10** Check the BGP configuration to see whether loopback interfaces are used to establish BGP peers.
 - If so, go to step 14.
 - If not, go to step 15.
- Step 11** Enter the view of the outbound interface, and run the **display this** command to check whether the interface is shut down.
 - If so, run the **undo shutdown** command to enable the interface.
 - If not, go to step 22.
- Step 12** Run the **display ospf peer** command to check whether the OSPF peer relationship is established.
 - If so, go to step 23.
 - If not, refer to the solution provided in the case of alarm OSPF_1.3.6.1.2.1.14.16.2.2 ospfNbrStateChange.
- Step 13** Run the **display isis peer** command to check whether the IS-IS peer relationship is established.
 - If so, go to step 23.
 - If not, refer to the solution provided in the case of alarm ISIS_1.3.6.1.3.37.2.0.13 isisRejectedAdjacency.
- Step 14** Check whether the **peer connect-interface** is configured for specifying the source address.
 - If so, go to step 15.
 - If not, go to step 16.
- Step 15** If BGP is the EBGP neighbor relationship and multiple hops exist between EBGP neighbors, check whether the **peer ebgp-max-hop** is configured.
 - If so, go to step 17.
 - If not, go to step 19.
- Step 16** Configure the **peer connect-interface** command. The parameter in the command must be the local interface that establishes a connection with the peer. Then, check whether the alarm BGP_1.3.6.1.4.1.2011.5.25.177.1.3.9 hwBgpPeerEstablished appears later.
 - If so, go to step 24.
 - If not, go to step 23.
- Step 17** Check whether the **peer valid-ttl-hops hops** command is configured.
 - If so, go to step 18.
 - If not, go to step 23.
- Step 18** If the **peer valid-ttl-hops hops** is configured, check whether the TTL of the packet to the peer ranges from [255-hops+1] to 255.

- If so, go to step 23.
- If not, go to step 20.

Step 19 Configure the **peer ebgp-max-hop**. Then, check whether the alarm BGP_1.3.6.1.4.1.2011.5.25.177.1.3.9 hwBgpPeerEstablished appears later.

- If so, go to step 24.
- If not, go to step 23.

Step 20 Change the value of the **peer valid-ttl-hops hops** and make it within the range from $[255-hops+1]$ to 255. Then, check whether the alarm BGP_1.3.6.1.4.1.2011.5.25.177.1.3.9 hwBgpPeerEstablished appears later.

- If so, go to step 24.
- If not, go to step 23.

Step 21 Run the **display cpu-usage** command to check whether the CPU usage remains 100% in a period.

- If so, go to step 23.
- If not, go to step 6.

Step 22 Contact the maintenance personnel of the peer device to check whether BGP is reset on the peer router, the peer is enabled in other address families on the local, and parameters for BGP connection are configured. Then, check whether the alarm BGP_1.3.6.1.4.1.2011.5.25.177.1.3.9 hwBgpPeerEstablished appears later.

- If so, go to step 24.
- If not, go to step 23.

Step 23 Collect alarm information and configuration information, and then contact technical support personnel.

Step 24 End.

----End

Clearing

After the certificate is deleted, the system clears this alarm, removing the need to manually clear it. This alarm will not be displayed on the **Current Alarms** page.

3.1.19 ALM-3491241990 The BGP Neighbor Is Disconnected

Description

BGP/2/HWBACKWARD:OID [OID] The BGP FSM moves from a higher numbered state to a lower numbered state. (InstanceId=[gauge], Afi=[integer], Safi=[integer], PeerType=[integer], PeerRemoteAddr=[binary], InterfaceIndex=[integer], PeerLastError=[octet], PeerState=[integer], PeerUnavaiReason=[gauge], InterfaceName=[octet])

This alarm is generated when the BGP state machine moved from a higher numbered state, namely, OpenConfirm or Established, to a lower numbered state.

Attribute

Alarm ID	OID	Alarm Severity	Alarm Type
34912 41990	1.3.6.1.4.1.2011.5.25 .177.1.3.10	Major	Communication alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
InstanceId	Indicates the index of the instance to which the peer belongs.
Afi	Indicates the address family: 1: ipv4 2: ipv6 25: vpls 196: l2vpn
Safi	Indicates the sub-address family: 1: unicast 2: multicast 4: mpls 65: vpls 128: vpn
PeerType	Indicates the address type of the peer: 1: ipv4 2: ipv6
PeerRemoteAddr	Indicates the address of the peer.
InterfaceIndex	Indicates the index of the interface.

Name	Meaning
PeerLastError	Indicates the error code of the BGP Notification when the neighbor relationship is disconnected for the last time. The value is expressed in the format of [ErrorCode][ErrorSubCode]. [ErrorCode] refers to the error code and [ErrorSubCode] refers to the error subcode. Take the integer 35 as an example, figure 3 is the error code and figure 5 is the error subcode. For detailed information about the error code, refer to BGP Error Code. If the value is 0, it indicates that no error occurs.

Name	Meaning
PeerState	Indicates the status of the BGP peer. • 1 Idle: indicates that BGP denies any request of entering. This is the initiatory status of BGP. Upon receiving a Start event, BGP initiates a TCP connection to the remote BGP peer, starts the ConnectRetry Timer with the initial value, listens for a TCP connection initiated by the remote BGP peer, and changes its state to Connect. • 2 Connect: indicates that BGP performs other actions after the TCP connection is set up. – If the TCP connection succeeds, BGP stops the ConnectRetry Timer, sends an Open message to the remote peer, and changes its state to OpenSent. – If the TCP connection fails, BGP restarts the ConnectRetry Timer with the initial value, continues to listen for a TCP connection initiated by the remote peer, and changes its state to Active. – If the ConnectRetry Timer has expired before a TCP connection is established, BGP restarts the timer with the initial value, initiates a TCP connection to the remote BGP peer, and stays in the Connect state. • 3 Active: indicates that BGP tries to set up TCP connection. This is the intermediate status of BGP. – If the TCP connection succeeds, BGP stops the ConnectRetry Timer, sends an Open message to the remote peer, and changes its state to OpenSent. – If the ConnectRetry Timer has expired before a TCP connection is established, BGP restarts the timer with the initial value and changes its state to Connect. – If BGP initiates a TCP connection with an unknown IP address, the

Name	Meaning
	TCP connection fails. When this occurs, BGP restarts the ConnectRetry Timer with the initial value and stays in the Active state. • 4 OpenSent: indicates that BGP has sent one Open message to its peer and waits for the other Open message from the peer. – If there are no errors in the Open message received, BGP changes its state to OpenConfirm. – If there are errors in the Open message received, BGP sends a Notification message to the remote peer and changes its state to Idle. – If the TCP connection fails, BGP restarts the ConnectRetry Timer with the initial value, continues to listen for a TCP connection initiated by the remote peer, and changes its state to Active. • 5 OpenConfirm: indicates that BGP waits for a Notification message or a Keepalive message. – If BGP receives a Notification message, or the TCP connection fails, BGP changes its state to Idle. – If BGP receives a Keepalive message, BGP changes its state to Established. • 6 Established: indicates that BGP peers can exchange Update, Notification and Keepalive packets. – If BGP receives an Update or a Keepalive message, its state stays in Established. – If BGP receives a Notification message, BGP changes its state to Idle.
PeerUnavaiReason	Indicates the reason that the BGP peer is down.

Name	Meaning
InterfaceName	Interface name. If the value of this parameter is NULL, the alarm is irrelevant with the interface.

Impact on the System

The BGP neighbor will be disconnected, and the BGP route received from the neighbor will be deleted. The packet forwarding based on the BGP route will fail.

Possible Causes

1. The BGP hold timer timed out and did not receive the Keepalive packet.
2. BGP received incorrect BGP packets or Notification packets from the neighbor.
3. The BGP neighbor relationship was reset and the neighbor relationship was automatically interrupted.

Procedure

Step 1 Check the link quality settings.

Log in to the iMaster NCE-Campus as a tenant administrator. Choose **Provision > Physical Network > Site Configuration** from the main menu, select the site to which the faulty device belongs, and click the **WAN Route** tab. On the tab page that is displayed, check the settings of **Keepalive time** and **Hold time**.

- If the settings are correct, no operation is required.
- If not, modify the parameters.

Step 2 Check the EBGp link encryption configuration.

1. Log in to the iMaster NCE-Campus as a tenant administrator. Choose **Provision > Virtual Network > Overlay Network** from the main menu, click the **Overlay Service** tab, and then click the **LAN Route** tab. On the tab page that is displayed, check whether the authentication type of BGP is configured.
 - a. If so, change the password and change the password on the BGP peer end accordingly.
 - b. If not, select the BGP configuration record of the faulty device, click the modification icon in the **Operation** column, and configure the authentication type.
2. Log in to the iMaster NCE-Campus as a tenant administrator. Choose **Provision > Physical Network > Site Configuration** from the main menu, select the site to which the faulty device belongs, and click the **WAN Route** tab. On the tab page that is displayed, check whether the authentication type of BGP is configured.
 - a. If so, change the password and change the password on the BGP peer end accordingly.

- b. If not, select the BGP configuration record of the faulty device, click the modification icon in the **Operation** column, and configure the authentication type.

Step 3 Run the **display bgp peer ipv4-address log-info** command to check the Error field in the command output. You can view the Error Code and Sub Error Code in the received Notification in the form of [ErrorCode][ErrorSubCode].

- If the error code of the Notification is 1, it indicates that the BGP module receives the packet with incorrect headers. Then, go to step 25.
- If the error code of the Notification is 2, it indicates that the BGP module receives the incorrect Open packet. Then, go to step 25.
- If the error code of the Notification is 3, it indicates that the BGP module receives the incorrect Update packet. Then, go to step 25.
- If the error code of the Notification is 4, it indicates that till the Holdtimer times out, the BGP module does not receive the Keepalive packet. Then, go to step 6.
- If the error code of the Notification is 5, it indicates that the finite state machine of the BGP module is faulty. Then, go to step 25.
- If the error code of the Notification is 6, go to step 4.
- If the error code of the Notification is 4 and error subcode is 6, it indicates that the BGP peer device proactively tears down the connection. Then go to step 25.

Step 4 If the error code of the Notification is 6, it indicates that BGP automatically closes the connection. Then, you need to run the **display bgp peer ipv4-address log-info** command to view the Notification field and check whether the Notification is sent by the router that generates the alarm.

- If "Send Notification" is displayed, it indicates that the local router actively sends the Notification. Then, go to step 5.
- If "Receive Notification" is displayed, it indicates that the local router receives the Notification. Then, go to step 24.

Step 5 Search for the **reset bgp all** and **reset bgp ipv4-address** commands in the user logs to check whether BGP is reset on the local end; or search for the **peer ipv4-address enable** command to check whether the peer is enabled in other address families on the local, or parameters for the BGP connection are configured.

- If so, it indicates that incorrect configurations cause the alarm, and thus no action is required. Then, go to step 26.
- If not, go to step 25.

Step 6 If the error code is 4, it indicates that the BGP disconnection is caused by the timeout of the Holdtimer. Then, you need to check whether the address of the BGP neighbor can be pinged successfully.

- If so, go to step 23.
- If not, go to step 7.

Step 7 Run the **display ip routing-table** command to check whether the Destination/Mask field has the route to the peer address.

- If so, go to step 9.
- If not, go to step 10.

- Step 8** Run the **display acl all** command to check whether the router is configured with the ACL that disables TCP port 179.
- If so, go to step 11.
 - If not, go to step 12.
- Step 9** Run the **display ip interface brief** command to check whether the values of Physical and Protocol fields of the outbound interface are Up.
- If so, go to step 25.
 - If not, go to step 13.
- Step 10** Check the origin of the route with the BGP peer address.
- If the route is originated from OSPF, go to step 14.
 - If the route is originated from IS-IS, go to step 15.
 - Else, go to step 25.
- Step 11** Delete the ACL that disables the TCP port 179, and check whether the alarm BGP_1.3.6.1.4.1.2011.5.25.177.1.3.9 hwBgpPeerEstablished appears later.
- If so, go to step 26.
 - If not, go to step 12.
- Step 12** Check the BGP configuration to see whether loopback interfaces are used to establish BGP peers.
- If so, go to step 16.
 - If not, go to step 17.
- Step 13** Enter the view of the outbound interface, and run the **display this** command to check whether the interface is shut down.
- If so, run the **undo shutdown** command to enable the interface.
 - If not, go to step 24.
- Step 14** Run the **display ospf peer** command to check whether the OSPF peer relationship is established.
- If so, go to step 25.
 - If not, refer to the solution provided in the case of alarm OSPF_1.3.6.1.2.1.14.16.2.2 ospfNbrStateChange.
- Step 15** Run the **display isis peer** command to check whether the IS-IS peer relationship is established.
- If so, go to step 25.
 - If not, refer to the solution provided in the case of alarm ISIS_1.3.6.1.3.37.2.0.13 isisRejectedAdjacency.
- Step 16** Check whether the **peer connect-interface** is configured for specifying the source address.
- If so, go to step 17.
 - If not, go to step 18.
- Step 17** If BGP is the EBGP neighbor relationship and multiple hops exist between EBGP neighbors, check whether the **peer ebgp-max-hop** is configured.
- If so, go to step 19.

- If not, go to step 21.
 - Step 18** Configure the **peer connect-interface** command. The parameter in the command must be the local interface that establishes a connection with the peer. Then, check whether the alarm BGP_1.3.6.1.4.1.2011.5.25.177.1.3.9 hwBgpPeerEstablished appears later.
 - If so, go to step 26.
 - If not, go to step 27.
 - Step 19** Check whether the **peer valid-ttl-hops hops** command is configured.
 - If so, go to step 20.
 - If not, go to step 25.
 - Step 20** If the **peer valid-ttl-hops hops** is configured, check whether the TTL of the packet to the peer ranges from $[255-hops+1]$ to 255.
 - If so, go to step 25.
 - If not, go to step 22.
 - Step 21** Configure the **peer ebgp-max-hop**. Then, check whether the alarm BGP_1.3.6.1.4.1.2011.5.25.177.1.3.9 hwBgpPeerEstablished appears later.
 - If so, go to step 26.
 - If not, go to step 25.
 - Step 22** Change the value of the **peer valid-ttl-hops hops** and make it within the range from $[255-hops+1]$ to 255. Then, check whether the alarm BGP_1.3.6.1.4.1.2011.5.25.177.1.3.9 hwBgpPeerEstablished appears later.
 - If so, go to step 26.
 - If not, go to step 25.
 - Step 23** Run the **display cpu-usage** command to check whether the CPU usage remains 100% in a period.
 - If so, go to step 25.
 - If not, go to step 8.
 - Step 24** Contact the maintenance personnel of the peer device to check whether BGP is reset on the peer router, the peer is enabled in other address families on the local, and parameters for BGP connection are configured. Then, check whether the alarm BGP_1.3.6.1.4.1.2011.5.25.177.1.3.9 hwBgpPeerEstablished appears later.
 - If so, go to step 26.
 - If not, go to step 25.
 - Step 25** Collect alarm information and configuration information, and then contact technical support personnel.
 - Step 26** End.
- End

Clearing

After the certificate is deleted, the system clears this alarm, removing the need to manually clear it. This alarm will not be displayed on the **Current Alarms** page.

3.1.20 ALM-4288421943 VM CPU Usage Exceeding the Threshold

Description

EVM/2/EVM_CPU_USAGE_RISING:OID [OID] VM CPU utilization exceeded the pre-alarm threshold.(VMName=\"[octet]\", ThresholdWarning=[INTEGER], Thresholdcurrent=[INTEGER])

The VM CPU usage exceeded the threshold.

Attribute

Alarm ID	OID	Alarm Severity	Alarm Type
4288421943	1.3.6.1.4.1.201.1.5.25.348.2.7.1	Major	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
VMName	Indicates a VM name.
ThresholdWarning	Indicates the alarm threshold.
Thresholdcurrent	Indicates the CPU usage.

Impact on the System

Services are affected.

Possible Causes

The configured VM specifications do not meet current service requirements.

Procedure

- Step 1** Based on the VM type, log in to the VM and check whether the total memory and CPU usage of all supported services are normal.
- If so, go to step 2.
 - If not, rectify the fault. If the fault persists, go to step 3.
- Step 2** Configure a VM with more CPUs or with a higher memory or reduce services. Check whether the alarm is cleared.
- If the alarm is cleared, go to step 4.
 - If the alarm persists, go to step 3.
- Step 3** Collect alarm information, log information, and configuration, and contact technical support personnel.
- Step 4** End.
- End

Clearing

After the fault is rectified, the system clears this alarm, removing the need to manually clear it. This alarm will not be displayed on the **Current Alarms** page.

3.1.21 ALM-4288421944 VM Memory Usage Exceeding the Threshold

Description

EVM/2/EVM_MEM_USAGE_RISING:OID [OID] VM Memory utilization exceeded the pre-alarm threshold.(VMName="\[octet]\", ThresholdWarning=[INTEGER], Thresholdcurrent=[INTEGER])

The VM memory usage exceeded the threshold.

Attribute

Alarm ID	OID	Alarm Severity	Alarm Type
4288421944	1.3.6.1.4.1.201.1.5.25.348.2.6.1	Major	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
VMName	Indicates a VM name.
ThresholdWarning	Indicates the alarm threshold.
Thresholdcurrent	Indicates the memory usage.

Impact on the System

Services are affected.

Possible Causes

The configured VM specifications do not meet current service requirements.

Procedure

- Step 1** Based on the VM type, log in to the VM and check whether the total memory and CPU usage of all supported services are normal.
- If so, go to step 2.
 - If not, rectify the fault. If the fault is still there, go to step 3.
- Step 2** Configure a VM with a higher memory or reduce services. Check whether the alarm is cleared.
- If the alarm is cleared, go to step 4.
 - If the alarm persists, go to step 3.
- Step 3** Collect alarm information, log information, and configuration, and contact technical support personnel.
- Step 4** End.
- End

Clearing

After the fault is rectified, the system clears this alarm, removing the need to manually clear it. This alarm will not be displayed on the **Current Alarms** page.

3.1.22 ALM-4288421945 VM State Exception

Description

EVM/2/EVM_ABNORMALLY_RUN:OID [OID] The VM is running abnormally.
(VMName="*octet*")

The VM is not working properly.

Attribute

Alarm ID	OID	Alarm Severity	Alarm Type
4288421945	1.3.6.1.4.1.201.1.5.25.19.2.2.0.2.1	Major	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
VMName	Indicates a VM name.

Impact on the System

Services are affected.

Possible Causes

The system file was deleted by mistake or a software bug existed.

Procedure

- Step 1** Install the VM again. Check whether the alarm is cleared.
 - If the alarm is cleared, go to step 3.
 - If the alarm persists, go to step 2.
- Step 2** Collect alarm information, log information, and configuration, and contact technical support personnel.
- Step 3** End.
- End

Clearing

The alarm needs to be cleared manually.

3.1.23 ALM-1880563716 The OSPF Neighbor Is Disconnected

Description

OSPF/2/NBRCHG:OID [OID]: The status of the non-virtual neighbor changes.
(NbrIpAddress=[neighbor-ip-address], NbrAddressLessIndex=[neighbor-interface-index], ProcessId=[process-id], AreaId=[area-id], IfnetIndex=[interface-ifnet-index], LocalIfIpAddress=[local-ip-address], ProcessId=[process-id], RouterId=[router-id], NbrRtrId=[neighbor-router-id], NbrState=[neighbor-state], IfName=[interface-name], InstanceName=[instance-name], NbrChgReason=[NbrStateChangeReason])

The status of the OSPF neighbor changed. The possible cause was that the status of the interface of the neighbor changed or the contents of the received Hello packets changed.

Attribute

Alarm ID	OID	Alarm Severity	Alarm Type
1880563716	1.3. 6.1. 2.1. 14. 16. 2.2	Major	environmentalAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
NbrIpAddress	Indicates the IP address of the neighbor.
NbrAddressLessIndex	Indicates the index of a neighboring interface.
ProcessId	Indicates the process ID.
AreaId	Indicates the area ID of the NSSA.
IfnetIndex	Indicates the Ifnet index of the interface.
LocalIfIpAddress	Indicates the IP address of the local router.
ProcessId	Indicates the process ID.

Name	Meaning
RouterId	Indicates the router ID of the local router.
NbrRtrId	Indicates the router ID of the neighbor.
NbrState	Indicates the status of the neighbor. • 1: Down • 2: Attempt • 3: Init • 4: 2Way • 5: ExStart • 6: Exchange • 7: Loading • 8: Full
IfName	Indicates the name of interface.
InstanceName	Indicates the instance name.
NbrChgReason	Indicates the reason why the neighbor status changes: • 1 (adjacencyHoldTimerExpired): indicates that the timer of the adjacent router times out. • 2 (physicalInterfaceChange): indicates that the status of the physical interface on the router changes. • 3 (ospfProtocolReason): indicates that an alarm is generated because of the OSPF protocol. • 4 (bfdSessionStateChange): indicates that the BFD session is closed. • 5 (configureChange): indicates that the OSPF configuration changes. • 6 (peerRouterReason): indicates that an alarm is generated because of the neighboring router. • 100 (alarmCleared): indicates that the alarm is cleared because services are restored or the neighbor is deleted.

Impact on the System

When the status of the neighbor (not a neighbor of a virtual link) changes, this alarm message will be sent. This alarm message indicates the status of the neighbor changes. If the neighbor changes from a lower status to a higher status, this alarm message is informational only, and no action is required. If the neighbor changes from a higher status to a lower status, services may be interrupted. (The state transition of the OSPF neighbor in an ascending order is: Down -> Init -> 2-way -> Exstart -> Exchange -> Loading -> Full).

Possible Causes

1. The status of the interface of the neighbor changed.
2. OSPF was restarted by using the **reset ospf process** command or the active/standby switchover was performed by using the **slave switchover** command.
3. An error packet was received.
4. The link between the OSPF neighbors is disconnected.

Procedure

- Step 1** Run the **display ospf peer** command to check the neighbor status. If the neighbor is in the Full state, go to step 7; otherwise, go to step 2.
- Step 2** Run the **display ip interface *interface-type interface-number*** command to check whether the interface of the neighbor is in the Down state.
- If the physical interface is Up, go to step 3.
 - If the physical interface is Down, check whether the **shutdown** command is configured on the interface and the link.
 - If this command is configured, run the **undo shutdown** command and then go to step 3.
 - If this command is not configured, go to step 8.
- Step 3** Check whether the packet is correctly forwarded and ping the IP address of the remote interface.
- If the ping fails, go to step 7.
 - If the ping succeeds, go to step 4.
- Step 4** Run the **display ospf interface *interface-type interface-number*** command to view the state field and check whether the interface where the OSPF neighbor resides is in the Down state.
- If the interface is in the Down state, go to step 7.
 - If the interface is in another state, go to step 5.
- Step 5** Run the **display ospf interface *interface-type interface-number*** command to check whether the configurations (including the hello interval, dead interval, poll interval, and OSPF network-type) on the two ends of the link are consistent and whether the interface on one end is not an OSPF interface.
- If so, go to step 6.
 - If not, modify the configurations to make them consistent. Then check whether the alarm is cleared.

- If so, go to step 6.
 - If not, run the following commands to modify interface configurations on the two ends to be consistent.
 - **ospf timer hello** *interval*
 - **ospf timer dead** *interval*
 - **ospf timer poll** *interval*
 - **ospf network-type** { **broadcast** | **nbma** | **p2mp** | **p2p** }
- Then, check whether the alarm is cleared.
- If so, go to step 8.
 - If not, go to step 7.

Step 6 Run the **display current-configuration interface** *interface-type interface-number* command to check whether the interface authentication configurations on the two ends are consistent.

- If so, go to step 7.
 - If not, run the following commands to modify interface configurations on the two ends to be consistent.
 - **ospf authentication-mode** { **simple** [**plain** *plain-text* | [**cipher**] *cipher-text*] | **null** }
 - **ospf authentication-mode** { **md5** | **hmac-md5** | **hmac-sha256** } [*key-id* { **plain** *plain-text* | [**cipher**] *cipher-text* }]
 - **ospf authentication-mode keychain** *keychain-name*
- Then, check whether the alarm is cleared.
- If so, go to step 8.
 - If not, go to step 7.

 NOTE

To ensure high security, it is recommended that the simple, md5, hmac-md5, and null authentication modes be not used.

Step 7 Collect alarm information and configuration information, and then contact technical support personnel.

Step 8 End.

----End

Clearing

After the fault is rectified, the system clears this alarm, removing the need to manually clear it. This alarm will not be displayed on the **Current Alarms** page.

3.1.24 ALM-4287766530 The CA certificate is nearly expired

Description

PKI/4/PKICACERTNEARLYEXPIRED: OID [OID] the CA certificate is nearly expired. (CACertIssuer=[issuer], CACertSubject=[subject], CACertStartTime=[starttime], CACertFinishTime=[finishtime])

The CA certificate is about to expire.

Attribute

Alarm ID	OID	Alarm Severity	Alarm Type
4287766530	1.3.6.1.4.1.201.1.6.122.34.0.2.11	Warning	Communication alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
issuer	Indicates the issuer of the CA certificate.
subject	Indicates the subject of the CA certificate.
starttime	Indicates the start time of the CA certificate.
finishtime	Indicates the end time of the CA certificate.

Impact on the System

The service will be invalid after the certificate expires.

Possible Causes

The CA certificate is about to expire. The CA certificate expiration time is less than the certificate expired prewarning time configured by the **pki set-certificate expire-prewarning** command.

Procedure

Step 1 Run the **display clock** command to check whether the device time is correct.

If not, run the **clock datetime** command in the user view to change the device time.

Step 2 Apply for a new certificate through SCEP or CMPv2 online or apply for a new certificate offline. For details, see "PKI Configuration" in the *Huawei AR1000V Product Documentation*.

----End

Clearing

After the fault is rectified, the system clears this alarm, removing the need to manually clear it. This alarm will not be displayed on the **Current Alarms** page.

3.1.25 ALM-4287766531 The local certificate is invalid

Description

PKI/2/PKILOCALCERTINVALID: OID [OID] the local certificate is invalid.
(LocalCertIssuer=[issuer], LocalCertSubject=[subject],
LocalCertStartTime=[starttime], LocalCertFinishTime=[finishtime])

The local certificate is invalid.

Attribute

Alarm ID	OID	Alarm Severity	Alarm Type
4287766531	1.3.6.1.4.1.201.1.6.122.34.0.2.12	Major	Communication alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
issuer	Indicates the issuer of the local certificate.
subject	Indicates the subject of the local certificate.

Name	Meaning
starttime	Indicates the start time of the local certificate.
finishtime	Indicates the end time of the local certificate.

Impact on the System

The service becomes invalid.

Possible Causes

The local certificate is invalid.

Procedure

Step 1 Check whether the system time on the local device is correct.

Step 2 If the system time is correct, apply for a new local certificate.

----End

Clearing

The alarm needs to be cleared manually.

3.1.26 ALM-4287766532 The Local Certificate Is About to Expire

Description

PKI/4/PKILOCALCERTNEARLYEXPIRED: OID [*OID*] the local certificate is nearly expired. (LocalCertIssuer=[*issuer*], LocalCertSubject=[*subject*], LocalCertStartTime=[*starttime*], LocalCertFinishTime=[*finishtime*])

The local certificate is about to expire.

Attribute

Alarm ID	OID	Alarm Severity	Alarm Type
4287766532	1.3.6.1.4.1.201.1.6.122.34.0.2.14	Warning	Communication alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
<i>issuer</i>	Indicates the issuer of the local certificate.
<i>subject</i>	Indicates the subject of the local certificate.
<i>starttime</i>	Indicates the start time of the local certificate.
<i>finishtime</i>	Indicates the end time of the local certificate.

Impact on the System

The service will be invalid after the certificate expires.

Possible Causes

The local certificate is about to expire. The local certificate expiration time is less than the certificate expired prewarning time configured by the **pki set-certificate expire-prewarning** command.

Procedure

Step 1 Check whether the system time on the local device is correct.

Step 2 If the system time is correct, apply for a new local certificate immediately.

----End

Clearing

The alarm needs to be cleared manually.

3.1.27 ALM-4287766533 The CRL Is Invalid

Description

PKI/2/PKICRLINVALID: OID [OID] the crl is invalid. (CrlIssuer=[crlissuer], CrlStartTime=[crlstarttime], CrlFinishTime=[crlfinishtime])

The CRL is invalid.

Attribute

Alarm ID	OID	Alarm Severity	Alarm Type
4287766533	1.3.6.1.4.1.201.1.6.122.34.0.2.15	Major	Communication alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
crlissuer	Indicates the issuer of the CRL.
crlstarttime	Indicates the start time of the CRL.
crlfinishtime	Indicates the end time of the CRL.

Impact on the System

The service becomes invalid.

Possible Causes

Indicates that the current system time is out of the CRL validity period.

Procedure

- Step 1** Run the **display clock** command to check whether the device time is correct.
If not, run the **clock datetime** command in the user view to change the device time.
- Step 2** Obtain a new CRL. For details, see "Configuring Local Certificate Check" in Huawei AR1000VV300R019 Configuration Guide - PKI Configuration.
- End

Clearing

After the fault is rectified, the system clears this alarm, removing the need to manually clear it. This alarm will not be displayed on the **Current Alarms** page.

3.1.28 ALM-4287766534 The CRL Is About to Expire

Description

PKI/4/PKICRLNEARLYEXPIRED: OID [*OID*] the *crl* is nearly expired.
(*CrlIssuer*=[*crlissuer*], *CrlStartTime*=[*crlstarttime*], *CrlFinishTime*=[*crlfinishtime*])
The CRL is about to expire.

Attribute

Alarm ID	OID	Alarm Severity	Alarm Type
4287766534	1.3.6.1.4.1.201.1.6.122.34.0.2.17	Warning	Communication alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
<i>crlissuer</i>	Indicates the issuer of the CRL.
<i>crlstarttime</i>	Indicates the start time of the CRL.
<i>crlfinishtime</i>	Indicates the end time of the CRL.

Impact on the System

The service becomes invalid.

Possible Causes

The CRL is to expire. The CRL expiration time is less than 2 hours ahead of the current system time.

Procedure

Step 1 Run the **display clock** command to check whether the device time is correct.

If not, run the **clock datetime** command in the user view to change the device time.

Step 2 Obtain a new CRL. For details, see "Configuring Local Certificate Check" in *Huawei AR1000VV300R019 Configuration Guide - PKI Configuration*.

----End

Clearing

After the fault is rectified, the system clears this alarm, removing the need to manually clear it. This alarm will not be displayed on the **Current Alarms** page.

3.1.29 ALM-157024261 The License Is About to Expire

Description

GTL/4/NEARDEADLINE:OID [OID] License feature [OCTET] is near deadline, remain time is [INTEGER] days, main board name is [OCTET].

The trap was generated when the system date was approaching the deadline of the service module defined in the license, that is, when the license entered the trial status.

Attribute

Alarm ID	OID	Alarm Severity	Alarm Type
157024261	1.3.6.1.4.1.201.1.5.25.142.2.3	Major	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
OCTET	Indicates the name of the resource item.
INTEGER	Indicates the number of remaining days.
OCTET	Indicates the name of main board.

Impact on the System

If the new license file is not applied for and activated before the probation period of the existing license file expires, the function items subject to the license will become unavailable and resource items will run as a smaller default value.

NOTE

This trap is reported once a day within the trial period.

Possible Causes

The license was approaching the deadline and soon would become invalid.

Procedure

- Step 1** This trap indicates that the current license file nearly reaches the deadline, and you should apply for the new license file before the deadline.
- Step 2** Use the new license file and run the **license active** *license-name* command to activate it.
- Step 3** Collect alarm information and configuration information, and then contact technical support personnel.

----End

Clearing

After the fault is rectified, the system clears this alarm, removing the need to manually clear it. This alarm will not be displayed on the **Current Alarms** page.

3.1.30 ALM-1098063877 NQA ICMP Test Failed

Description

NQA/4/PINGFAIL:OID [OID] Ping entry test failed. (Admin=[OCTET], Tag=[OCTET])

The trap was generated when the number of continuous test failures reached the threshold. The default threshold was 1. You can run the **test-failtimes** command to modify the threshold.

Attribute

Alarm ID	OID	Alarm Severity	Alarm Type
1098063877	1.3.6.1.2.1.80.0.2	Warning	Communication alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
Admin	Indicates the index of the test administrator.
Tag	Indicates the index of the test name.

Impact on the System

None

Possible Causes

This trap occurred in the NQA test.

1. The destination address was inexistent and the route was unreachable.
2. The destination address existed, but the route was unreachable.
3. Because of the network delay, the RTT of the packet was longer than the set timeout period.

Procedure

Step 1 Run the **display this** command in the NQA test view to check whether the destination address is correctly configured. If not, run the **destination-address** command in the NQA test view to modify the destination address.

Perform the test again to check whether the alarm is cleared.

- If so, go to Step 5.
- If not, go to Step 2.

Step 2 Run the **ping** command in the NQA test view to check whether the route is reachable.

- If the destination address is correctly configured, but the route is not reachable, run the **display ip routing-table** command to check the routing table and rectify the routing fault. If the test fails again, go to Step 4.
- If the route is reachable, go to Step 3.

Step 3 Run the **timeout** command in the NQA test view to modify the timeout period according to the status of the current network. It is recommended that you modify the timeout period to the default value, that is, three seconds. The value of the timeout period ranges from 1 second to 60 seconds. You can run the **display this** command in the NQA test view to view the current timeout period.

Perform the test again to check whether the alarm is cleared.

- If so, go to Step 5.
- If not, go to Step 4.

Step 4 Run the **display ospf interface** *interface-type interface-number* command and view the **State** field to check whether the interface where the OSPF neighbor is configured is in the Down state.

- If the interface is in the Down state, go to to Step 6.
- If the interface is in another state, go to step 5.

Step 5 Collect alarm information and configuration information, and then contact technical support personnel.

Step 6 End.

----End

Related Information

None

3.1.31 ALM-3491242000 The number of BGP routes exceeded the maximum number that is allowed

Description

BGP/3/HWBGPROUTEMAXEXCEED:OID [OID] The number of BGP routes exceeded the maximum number. (RouteTypeIndex=[integer], MaximumNumber=[integer])

The number of BGP routes exceeded the maximum number that is allowed.

Attribute

Alarm ID	OID	Alarm Severity	Alarm Type
3491242000	1.3.6.1.4.1.201.1.5.25.177.1.3.13	Major	Quality of service alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
RouteTypeIndex	Index of the BGP route type - IPv4: IPv4 routes, including IPv4 public network and IPv4 VPN routes - IPv4 Public: IPv4 public network routes - IPv4 VRF: IPv4 VPN routes - IPv6: IPv6 routes, including IPv6 public network and IPv6 VPN routes - IPv6 Public: IPv6 public network routes - IPv6 VRF: IPv6 VPN routes - L2AD: BGP L2VPN-AD routes
MaximumNumber	Maximum number of BGP routes of a specified type

Impact on the System

BGP routes will no longer be accepted. As a result, services will be affected.

Possible Causes

The number of BGP routes exceeded the maximum number that is allowed.

Procedure

- Step 1** Check whether this alarm is caused by configuration or topology errors.
- If this alarm is caused by configuration or topology errors, go to Step 2.
 - If this alarm is not caused by configuration or topology errors, go to Step 3.
- Step 2** Correct the configuration or topology errors.
- If the number of BGP routes falls below the maximum number that is allowed after the configuration or topology errors are corrected, go to Step 4.
- Step 3** If all the routes are necessary, determine whether to implement capacity expansion and contact technical support personnel.
- Step 4** End.
- End

Related Information

None

3.1.32 ALM-3491242001 The ratio of BGP routes to the maximum number that is allowed exceeded the alarm threshold

Description

BGP/3/HWBGPROUTETHRESHOLDEXCEED:OID [OID] The number of BGP routes exceeded the threshold. (RouteTypeIndex=[integer], CurrentRouteNumber=[integer], RouteThreshold=[integer], MaximumNumber=[integer])

The ratio of BGP routes to the maximum number that is allowed exceeded the alarm threshold.

Attribute

Alarm ID	OID	Alarm Severity	Alarm Type
3491242001	1.3.6.1.4.1.201.1.5.25.177.1.3.11	Minor	Quality of service alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
RouteTypeIndex	Index of the BGP route type • IPv4: IPv4 routes, including IPv4 public network and IPv4 VPN routes • IPv4 Public: IPv4 public network routes • IPv4 VRF: IPv4 VPN routes • IPv6: IPv6 routes, including IPv6 public network and IPv6 VPN routes • IPv6 Public: IPv6 public network routes • IPv6 VRF: IPv6 VPN routes • L2AD: BGP L2VPN-AD routes
CurrentRouteNumber	Current number of BGP routes of a specified type
RouteThreshold	Alarm threshold for the number of BGP routes of a specified type
MaximumNumber	Maximum number of BGP routes of a specified type

Impact on the System

The number of routes is approaching the maximum number that is allowed, and routes will no longer be accepted if the maximum number is reached, affecting services.

Possible Causes

The ratio of BGP routes to the maximum number that is allowed exceeded the alarm threshold.

Procedure

- Step 1** Check whether this alarm is caused by configuration or topology errors.
- If this alarm is caused by configuration or topology errors, go to Step 2.
 - If this alarm is not caused by configuration or topology errors, go to Step 3.

- Step 2** Correct the configuration or topology errors.

If the number of BGP routes falls below the maximum number that is allowed after the configuration or topology errors are corrected, go to Step 4.

- Step 3** If all the routes are necessary, determine whether to implement capacity expansion and contact technical support personnel.
- Step 4** End.
- End

Related Information

None

3.1.33 ALM-3276800300 The session resources were overloaded

Description

FWDTRAP/2/SESSIONRESLACK:OID [OID] The device session resources were overloaded.(Usage = [INTEGER]%)

The number of forwarding flow tables on the device reaches or exceeds 90% or 100% of the maximum number, an alarm is generated.

 NOTE

If the number of forwarding flow tables changes too rapidly within a short period of time, multiple alarms may be generated. As a result, the system records these alarms, affecting normal services on the device. To prevent the device from recording a large number of alarms, the system suppresses the alarms by setting the interval at which alarms are sent to longer than 30 minutes. That is, the system records an alarm at least 30 minutes after the last alarm was cleared.

Attribute

Alarm ID	OID	Alarm Severity	Alarm Type
3276800300	1.3.6.1.4.1.201.1.5.25.227.2.1.36	Major	Equipment alarm

Parameters

Name	Meaning
[OID]	Indicates the MIB object ID of the alarm.

Name	Meaning
Usage	The proportion that the number of forwarding flow tables on the device accounts for of the maximum number.

Impact on the System

Services are affected.

Possible Causes

The number of forwarding flow tables on the device reaches or exceeds 90% or 100% of the maximum number.

Procedure

Check service configurations and contact technical support personnel.

Related Information

None

3.1.34 ALM-3276800301 The evpn connection has entered the down state

Description

CONN/2/CONN_STATUS_DOWN:OID [OID] The connection has entered the down state. (ConnectionID = [integer1], SrcSiteID = [integer2], SrcTNPID = [integer3], DestSiteID = [integer4], DestTNPID = [integer5])

The iMaster NCE-Campus EVPN link is unavailable.

Attribute

Alarm ID	OID	Alarm Severity	Alarm Type
3276800301	1.3.6.1.4.1.201.1.5.25.241.6.3.2	Major	Communication alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
integer1	Indicates the link index.
integer2	Indicates the source site ID.
integer3	Indicates the source TNP ID.
integer4	Indicates the destination site ID.
integer5	Indicates the destination TNP ID.

Impact on the System

The system will not be affected.

Possible Causes

Cause 1:

No keepalive packet was received from the remote device within the configured detection period.

Cause 2:

The protocol status of a physical interface changed.

Cause 3:

The BGP connection between the local and remote sites was interrupted.

Procedure

Step 1 Check whether the interfaces bound to the TNPs can ping each other successfully.

- If so, go to [3](#).
- If not, go to [2](#).

Step 2 Check whether the intermediate transmission network is faulty.

Step 3 Collect log and configuration information, and contact technical support.

----End

Related Information

None

3.1.35 ALM-3276800302 The number of evpn connections has reached the maximum number

Description

CONN/2/CONN_MAX_EXCEED:OID [OID] The number of connections has reached the maximum number. (MaximumNumber = [integer1], KeepaliveInterval = [integer2])

The number of iMaster NCE-Campus EVPN connections reached the maximum value.

Attribute

Alarm ID	OID	Alarm Severity	Alarm Type
3276800302	1.3.6.1.4.1.2011.5.25.241.6.3.3	Major	Quality of service alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
integer1	Indicates the maximum number of connections supported by the device.
integer2	Indicates the keepalive interval.

Impact on the System

Links of some sites may be disconnected.

Possible Causes

Cause 1:

The configured keepalive interval was too short to support the current number of connections.

Cause 2:

There are a large number of sites, and the local device needs to establish connections with all sites. As a result, the number of connections to be established exceeds the maximum value supported by the device.

Procedure

- Step 1**
Check whether the keepalive interval is too short. If so, increase the keepalive interval and check whether the alarm is cleared.
 - If so, go to 4.
 - If not, go to 2.
- Step 2**
On the controller, adjust the inter-site topology, connect the local site to the hub site, and enable the hub site to forward packets. Then check whether a clear alarm is generated.
 - If so, go to 4.
 - If not, go to 3.
- Step 3**
Collect log and configuration information, and contact technical support.
- Step 4**
End.
- End

Related Information

None

3.1.36 ALM-3276800303 Power is unusable

Description

ENTITYTRAP/1/POWERUNUSEABLE:OID [OID] Power change to unusable status. (Index=[INTEGER1], EntityPhysicalIndex=[INTEGER2], PhysicalName="[OCTET]", EntityTrapFaultID=[INTEGER3])

The power supply is unavailable.

NOTE

Only the switch models with dual power supplies support this alarm.

Attribute

Alarm ID	OID	Alarm Severity	Alarm Type
3276800303	1.3.6.1.4.1.201.1.5.25.219.2.5.7	Critical	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
Index	Indicates an entity index.
EntityPhysicalIndex	Indicates a physical index.
PhysicalName	Indicates a physical entity name.
EntityTrapFaultID	Indicates the fault ID.

Impact on the System

Services are interrupted.

Possible Causes

- Cause 1: The device's power cable was removed.
- Cause 2: A power module was faulty.

Procedure

- Step 1** Check whether the power cable is removed.
- Step 2** If the power cable is working properly, check whether the power module is working properly.
- Step 3** If the power module is working properly, upgrade the system software or patch software to the latest version.
- Step 4** Collect alarm and configuration information, and contact technical support personnel.
- End

Related Information

None

3.1.37 ALM-3276800304 The number of connections has reached the threshold value

Description

CONN/4/CONN_THRESHOLD_EXCEED:OID [OID] The number of connections has exceeded the threshold. (CurrentConnecionNumber = [integer1], KeepaliveInterval = [integer2], ThresholdPercent = [integer3], MaximumNumber = [integer4])

The number of iMaster NCE-Campus EVPN connections reached the upper limit.

Attribute

Alarm ID	OID	Alarm Severity	Alarm Type
3276800304	1.3.6.1.4.1.201 1.5.25.241.6.3. 5	Minor	Quality of service alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
integer1	Indicates the number of current connections on the device.
integer2	Indicates the interval for detecting keepalive packets.
integer3	Indicates the upper threshold percentage of the link usage.
integer4	Indicates the maximum number of connections supported by the device.

Impact on the System

Users may fail to establish new connections.

Possible Causes

- Cause 1: The configured keepalive interval was too short, resulting in a small number of connections that the device can support.
- Cause 2: There are a large number of sites, and the local device needs to establish connections with all sites. As a result, the number of connections to be established exceeds the threshold value set by the device.

Procedure

- Step 1** Check whether the power cable is removed. Check whether the keepalive interval is too short. If so, increase the keepalive interval and check whether the alarm is cleared.
- Y=>4.
 - N=>2.
- Step 2** On the controller page, adjust the inter-site topology, connect the local site to the hub site, and enable the hub site to forward packets. Then check whether a clear alarm is generated. If the power module is working properly, upgrade the system software or patch software to the latest version.

- Y=>4.
- N=>3.

Step 3 Collect alarm and configuration information, and contact technical support personnel.

Step 4 End.

----End

Related Information

None

3.1.38 ALM-3276800306 The ms-channel has entered the down state

Description

MSCHANNEL/4/MSCHANNEL_STATUS_DOWN:OID [OID] The ms-channel has entered the down state.

The iMaster NCE-Campus active and standby channels enter the inactive state, and the internal communication links of two devices are unavailable.

Attribute

Alarm ID	OID	Alarm Severity	Alarm Type
3276800306	1.3.6.1.4.1.201 1.5.25.241.8.1. 2	Critical	Communication alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.

Impact on the System

The active and standby channels fail, and the internal communication links of the two iMaster NCE-Campus devices fail. As a result, a large number of BGP routes flap.

Possible Causes

The internal communication links between two iMaster NCE-Campus devices are disconnected, and heartbeat packets are lost.

Procedure

- Step 1** Run the **display interface** command to check whether the status and configurations of the interfaces between the internal communication links of the iMaster NCE-Campus devices are correct.
- If so, go to step 2.
 - If not, ensure that the interfaces are in the Up state and their IP addresses and routes are correctly configured.
- Step 2** Check whether heartbeat packets are lost due to heavy service traffic.
- If so, reduce unnecessary service traffic.
 - If not, go to step 3.
- Step 3** Collect alarm and configuration information, and contact technical support personnel.
- End

Related Information

None

3.1.39 ALM-3276800320 Fan Is Invalid

Description

ENTITYTRAP/4/FANINVALID:OID [OID] Fan is invalid.(Index=[INT1], EntityPhysicalIndex=[INT2], PhysicalName="[OCTET]", EntityTrapFaultID=[INT3])

The alarm is generated when fans become faulty.

Attribute

Alarm ID	OID	Alarm Severity	Alarm Type
3276800320	1.3.6.1.4.1.201.1.5.25.219.2.6.5	Warning	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
Resource ID	Indicates the resource ID of an entity.
Entity physical index	Indicates the sub-index of an entity.
Physical name	Indicates the name of an entity.
EntityTrapFaultID	Indicates the error code of the alarm.

Impact on the System

The temperature of boards becomes high.

Possible Causes

Fans are faulty. For example, fans stop rotating.

Procedure

- Run the **display fan** command to check the fan status. Check whether the fan tray is registered and the fan speed is zero.
 - If the fan tray is not registered, remove and install the fan tray.
 - If the fan speed is zero, replace the fan.If the fault persists, contact technical support personnel.

----End

Related Information

None

3.1.40 ALM-3276800321 Fan Has Been Removed

Description

ENTITYTRAP/4/FANREMOVE:OID [OID] Fan has been removed.(Index=[INT1], EntityPhysicalIndex=[INT2], PhysicalName="[OCTET]", EntityTrapFaultID=[INT3])

This alarm is generated when a fan module is removed.

Attribute

Alarm ID	OID	Alarm Severity	Alarm Type
3276800321	1.3.6.1.4.1.201.1.5.25.219.2.6.1	Warning	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
Resource ID	Indicates the resource ID of an entity.
Entity physical index	Indicates the sub-index of an entity.
Physical name	Indicates the name of an entity.
EntityTrapFaultID	Indicates the error code of the alarm.

Impact on the System

The temperature of boards becomes high.

Possible Causes

The fan is removed.

Procedure

Run the **display fan** command to check whether the fan is working properly. If not, remove and install the fan tray to ensure that it is well connected. If the fault persists, Collect alarm information and configuration information, and then contact technical support personnel.

Related Information

None

3.1.41 ALM-3276800322 The Power Module Is Removed

Description

ENTITYTRAP/4/POWERREMOVE: OID [OID] Power has been removed.
(Index=[INTEGER], EntityPhysicalIndex=[INTEGER], PhysicalName="[OCTET]", EntityTrapFaultID=[INTEGER])

The power supply unit was removed.

Attribute

Alarm ID	OID	Alarm Severity	Alarm Type
3276800322	1.3.6.1.4.1.201.1.5.25.219.2.5.1	Warning	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
Index	Indicates the index.
EntityPhysicalIndex	Indicates the physical entity index.
PhysicalName	Indicates the physical entity name.
EntityTrapFaultID	Indicates the error code.

Impact on the System

Boards cannot be powered on because power is insufficient.

Possible Causes

The power supply unit was removed.

Procedure

- Step 1** Check whether the power supply unit was removed manually.
- If so, no action is required.
 - If not, reinstall the power supply unit and go to step 2.
- Step 2** Run the **display power** command to check whether the power supply unit is present.
- If so, replace the power supply unit.
 - If not, go to step 4.
- Step 3** End.
- Step 4** Collect alarm information and configuration information, and then contact technical support personnel.

----End

Related Information

None

3.1.42 ALM-303046420 RDB restore have failed Report

Description

NAAS/2/NAAS_RDB_RESTROE_FAILED: OID [oid] The rdb recovery, some nodes may failed to be resotre.(XPATH failed result number = [*integer*]).

RDB restore have failed Report

Attribute

Alarm ID	OID	Alarm Severity	Alarm Type
303046420	1.3.6.1.4.1.2011.5.25.19.2.40	Major	Processing error alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
<i>integer</i>	Number of YANG nodes that fail to be restored. The value is an integer greater than or equal to 1.

Impact on the System

Services on the interface board fail to work.

Possible Causes

An interface card is removed during the restart, causing the failure to restore the RDB.

Procedure

1. If an interface card has been removed before the restart, install the interface card and restart the device.

Related Information

None

3.1.43 ALM-303046419 SPR Site Link Degrade

Description

SPR/4/SITELINKDEGRADE:OID [oid] SPR detects site link degrade. DestSite = [integer], VPNInstance = [string], AppPolicy = [integer], WorstLinkLoss = [integer], WorstLinkDelay = [integer], WorstLinkJitter = [integer], BestLinkLoss = [integer], BestLinkDelay = [integer], BestLinkJitter = [integer].

No link meets SLA requirements.

Attribute

Alarm ID	OID	Alarm Severity	Alarm Type
303046419	1.3.6.1.4.1.2011.5.25.241.2.4.3	Major	Quality of service alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
DestSite	Indicates the destination site.
VPNInstance	Indicates a VPN instance.
AppPolicy	Indicates the index of an application policy.
WorstLinkLoss	Indicates the packet loss rate of the worst link.

Name	Meaning
WorstLinkDelay	Indicates the delay of the worst link.
WorstLinkJitter	Indicates the jitter of the worst link.
BestLinkLoss	Indicates the packet loss rate of the best link.
BestLinkDelay	Indicates the delay of the best link.
BestLinkJitter	Indicates the jitter of the best link.

Impact on the System

Traffic transmission is affected.

Possible Causes

The quality of all links does not meet the SLA requirements.

Procedure

- 1. Run the **display sla detect result all** command to check all SLA statistics.
- 2. Collect alarm, log, and configuration information, and contact technical support personnel.
- 3. End.

Related Information

None

3.1.44 ALM-3235651584 MIB Information Change

Description

ENTMIB/4/TRAP:OID [oid] Entity MIB changes.

The MIB information changes because an entity (a board or a subcard) in a device is installed, removed, reset, or registered.

Attribute

Alarm ID	OID	Alarm Severity	Alarm Type
3235651584	1.3.6.1.2.1.47.2.0.1	Warning	Equipment alarm

Parameters

Name	Meaning
[oid]	Indicates the MIB object ID of the alarm.

Impact on the System

If the board is removed or reset, traffic collection on an interface may be affected, causing incorrect accounting.

Possible Causes

An entity (a board or a subcard) on a device is installed, removed, reset, or registered.

Procedure

Collect alarm information and configuration information, and then contact technical support personnel.

Related Information

None

3.1.45 ALM-3236306944 IPv6 Interface Status Change

Description

IPV6/2/IF_IPV6CHANGE:OID [oid] The status of the IPv6 Interface changed. (IfIndex=[INTEGER], IfDescr=[OCTET], IfOperStatus=[INTEGER], IfAdminStatus=[INTEGER])

The status of the IPv6 interface was changed.

Attribute

Alarm ID	OID	Alarm Severity	Alarm Type
3236306944	1.3.6.1.2.1.55.2.0.1	Major	Communication alarm

Parameters

Name	Meaning
oid	Indicates the MIB object ID of the alarm.

Name	Meaning
IfIndex	Indicates the index of the interface.
IfDescr	Indicates the description of the interface.
IfOperStatus	Indicates the current operating status of the interface. The value can be: up(1), down(2), and testing(3). • The value testing(3) indicates that the interface cannot forward any operational packets. • If the value of ifAdminStatus is down(2), the value of ifOperStatus is also down(2). • If the value of ifAdminStatus becomes up(1) and the interface can transmit and receive data, the value of ifOperStatus also becomes up(1). • If an error that prevents the interface from going Up occurs, the value of ifOperStatus remains down(2). Currently, the value testing(3) is not supported.
IfAdminStatus	Indicates the desired status of the interface. The value can be: up(1), down(2), and testing(3). The value testing(3) indicates that the interface cannot forward any operational packets. When a managed system initializes, all interfaces start with ifAdminStatus in the down(2) state. As a result of either management or configuration, the value of ifAdminStatus is changed to either up(1) or testing(3), or remains down(2) if not changed. Currently, the value testing(3) is not supported.

Impact on the System

The influence depends on the ipv6IfOperStatus:

1. Up: indicates that the IPv6 services on the interface are recovered.

2. Down: indicates that the IPv6 services on the interface are interrupted.

Possible Causes

- The protocol status on the interface became Down.
 - Cause 1: The interface was damaged or the link was faulty.
 - Cause 2: The interface was shut down.
 - Cause 3: When the IPv6 protocol was Up, the **undo ipv6 enable** command was run.
 - Cause 4: All the IPv6 addresses were deleted.
 - Cause 5: When the IPv6 protocol was Up, the IPv6 function was disabled.
- The interface protocol can become Up only when the following requirements are met synchronously.
 - Cause 1: The interface and the link are normal.
 - Cause 2: The **undo shutdown** command is run on the interface.
 - Cause 3: The IPv6 function is enabled in the system view.
 - Cause 4: The IPv6 forwarding function is enabled in the interface view.
 - Cause 5: The IPv6 address is assigned.

Procedure

1. If the interface turned Up, this log message is informational only and no action is required.
2. If the protocol status of the interface becomes Down, do as follows to locate the fault or change the protocol status to Up.
 - a. Run the **display ipv6 interface** [*interface-type interface-number*] command to check whether the IPv6 address is assigned to the interface.
 - If so, go to Step b.
 - If not, go to Step c.
 - b. Check the "current state" field of the interface in the **display ipv6 interface** [*interface-type interface-number*] command output.
 - If it displays Down, check whether the **shutdown** command is run on the remote interface.
 - If so, run the **undo shutdown** command in the remote interface view and then repeat Step a and Step b.
 - If not, it indicates that the local interface is damaged or the link is faulty. You need to replace the interface module or the cable, and then repeat Step a and Step b.
 - If it displays Administratively Down, run the **undo shutdown** command in the interface view, and then repeat Step a and Step b.
 - If it displays Up and the IPv6 protocol status is Down, go to Step e.
 - If it displays Up and the IPv6 protocol status is Up, go to Step i.
 - c. Run the **display this** command in the interface view to check whether the **ipv6 enable** command is configured.

- If so, go to Step d.
- If not, configure the **ipv6 enable** command. Then, go to Step d.
- d. Run the **ipv6 address** *ipv6-address prefix-length* in the interface view to assign the IPv6 address. Then, go to Step f.
- e. Run the **display this** command in the system view to check whether the **ipv6** command is configured.
 - If so, go to Step f.
 - If not, configure the **ipv6** command in the system view. Then, go to Step f.
- f. Run the **display ipv6 interface** [*interface-type interface-number* | **brief**] command to check the protocol status of the interface.
 - If the status is Down, go to Step g.
 - If the status is Up, go to Step h.
- g. Collect alarm information and configuration information, and then contact Huawei technical support personnel. Collect alarm information and configuration information, and then contact technical support personnel. Collect alarm information and configuration information, and then contact technical support personnel.
- h. End.

3.1.46 ALM-3244957696 IP Address Change

Description

IP/4/IP_TRAPID_IPADDRESSCHANGE:OID [oid] An IP address has been changed. (OldIpAddress=[IPADDR], NewIpAddress=[IPADDR], IfIndex=[INTEGER], OldIpMask=[IPADDR], NewIpMask=[IPADDR], InterfaceName=[STRING])

An alarm was generated when the primary IP address of an interface was manually changed.

Attribute

Alarm ID	OID	Alarm Severity	Alarm Type
3244957696	1.3.6.1.4.1.2011.5.25.41.6.1	Warning	Communication alarm

Parameters

Name	Meaning
oid	Indicates the MIB object ID of the alarm.

Name	Meaning
OldIpAddress	Original IP address
NewIpAddress	New IP address
IfIndex	Interface index
OldIpMask	Original IP address mask
NewIpMask	New IP address mask
InterfaceName	Interface name

Impact on the System

If the IP address is changed, services may be interrupted.

Possible Causes

The primary IP address of an interface was manually changed.

Procedure

The alarm is informational only, and no action is required.

Related Information

None

3.1.47 ALM-4285734912 IPSec tunnel start

Description

IPSEC/4/IPSECTUNNELSTART: OID [*oid*] The IPSec tunnel is established.
(Ifindex=[*Ifindex*], SeqNum=[*SeqNum*],TunnelIndex=[*TunnelIndex*],
RuleNum=[*RuleNum*], DstIP=[*DstIP*], InsidIP=[*InsidIP*],
RemotePort=[*RemotePort*], CpuID=[*CpuID*], SrcIP=[*SrcIP*], FlowInfo=[*FlowInfo*],
LifeSize=[*LifeSize*], LifeTime=[*LifeTime*], VsysName=[*vsys-name*],
InterfaceName=[*InterfaceName*], SlotID=[*SlotID*], Role=[*Role*])

An IPSec tunnel is established.

Attribute

Alarm ID	OID	Alarm Severity	Alarm Type
4285734912	1.3.6.1.4.1.2011.6. 122.26.6.1	Warning	Communication alarm

Parameters

Name	Meaning
oid	Indicates the MIB object ID of the alarm.
Ifindex	Indicates the interface index.
SeqNum	Indicates the policy number.
TunnelIndex	Indicates the tunnel index.
RuleNum	Indicates the rule number.
DstIP	Indicates the IP address of the peer end of the IPSec tunnel.
InsideIP	Indicates the intranet IP address of the peer end of the tunnel.
RemotePort	Indicates the port number of the peer end of the IPSec tunnel.
CpuID	Indicates the CPU number.
SrcIP	Indicates the IP address of the local end of the IPSec tunnel.
FlowInfo	Indicates the data flow information of the IPSec tunnel, including the source address, destination address, ACL port number, ACL protocol number, and DSCP.
LifeSize	Indicates the life cycle of the tunnel, in kbytes.
LifeTime	Indicates the life cycle of the tunnel, in seconds.
vsys-name	Indicates the name of the virtual system to which the IPSec policy belongs. NOTE The device does not support this parameter.
InterfaceName	Indicates the interface name.
SlotID	Indicates the Slot number. NOTE The device does not support this parameter.

Name	Meaning
Role	Device role during SA negotiation: • Initiator: The device functions as the SA negotiation initiator. • Responder: The device functions as the SA negotiation responder.

Impact on the System

None

Possible Causes

When an IPsec tunnel is established successfully, the alarm is generated. Procedure This trap message is informational only, and no action is required.

Related Information

None

3.1.48 ALM-4285734925 IPsec Negotiation Fails

Description

IPSEC/4/IPSECNEGOFAIL: OID [*OID*] IPsec tunnel negotiation fails.
(Ifindex=[*Ifindex*], SeqNum=[*SeqNum*], Reason=[*Reason*],
ReasonCode=[*ReasonCode*], PeerAddress=[*PeerAddress*], PeerPort=[*PeerPort*],
VsysName=[*vsys-name*], InterfaceName=[*InterfaceName*])

IPsec tunnel negotiation fails.

Attribute

Alarm ID	OID	Alarm Severity	Alarm Type
4285734925	1.3.6.1.4.1.2011.6.122.26.6.14	Warning	Communication alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.

Name	Meaning
Ifindex	Indicates the index of the interface on the IPsec tunnel.
SeqNum	Indicates the sequence number of the IPsec policy.
Reason	Indicates the reason of IPsec tunnel negotiation failure.

Name	Meaning
ReasonCode	Indicates the reason code of IPSec tunnel negotiation failure. • 1: phase1 proposal mismatch • 2: phase2 proposal or pfs mismatch • 3: encapsulation mode mismatch • 4: flow or peer mismatch • 5: version mismatch • 6: responder dh mismatch • 7: initiator dh mismatch • 10: ip assigned fail • 12: peer address mismatch • 13: config ID mismatch • 14: construct local ID fail • 15: authentication fail • 16: rekey no find old sa • 17: rekey fail • 18: first packet limited • 21: invalid cookie • 24: invalid length • 26: unsupported version • 28: malformed payload • 30: malformed message • 31: cookie mismatch • 32: exchange mode mismatch • 33: unknown exchange type • 34: critical drop • 35: uncritical drop • 36: route limit • 39: local address mismatch • 40: nat detection fail • 41: ipsec tunnel number reaches limitation • 42: dynamic peers number reaches limitation • 43: none of user's interface is selected • 44: in disconnect state • 45: proposal mismatch or use sm in ikev2 • 46: flow conflict

Name	Meaning
	• 47: ikev2 not support sm in ipsec proposal • 48: netmask mismatch • 49: no policy applied on interface • 50: fragment packet limit • 51: fragment packet reassemble timeout
PeerAddress	Indicates the remote IP address.
PeerPort	Indicates the remote UDP port number.
vsys-name	Indicates the name of the virtual system to which the IPSec policy belongs. NOTE The device does not support this parameter.
InterfaceName	Indicates the interface name.
ConnID	Indicates the connection ID of an SA.

Impact on the System

Creating an IPSec tunnel will fail.

Possible Causes

The possible causes are as follows:

- phase1 proposal mismatch: IKE proposal parameters of the two ends do not match.
- phase2 proposal or pfs mismatch: IPSec proposal parameters, pfs algorithm, or security ACL of the two ends do not match.
- responder dh mismatch: The DH algorithm of the responder does not match.
- initiator dh mismatch: The DH algorithm of the initiator does not match.
- encapsulation mode mismatch: The encapsulation mode does not match.
- flow or peer mismatch: The security ACL or IKE peer address of the two ends does not match.
- version mismatch: The IKE version number of the two ends does not match.
- peer address mismatch: The IKE peer address of the two ends does not match, or the VPN instance name specified during IKE negotiation is different from the VPN instance bound to the physical interface for IPSec tunnel negotiation.
- config ID mismatch: The IKE peer of the specified ID is not found.

- exchange mode mismatch: The negotiation mode of the two ends does not match.
- authentication fail: Identity authentication fails.
- construct local ID fail: The local ID fails to be constructed.
- rekey no find old sa: The old SA is not found during re-negotiation.
- rekey fail: The old SA is going offline during re-negotiation.
- first packet limited: The rate of the first packet is limited.
- unsupported version: The IKE version number is not supported.
- malformed message: Malformed message.
- malformed payload: Malformed payload.
- critical drop: Unidentified critical payload.
- cookie mismatch: Cookie mismatch.
- invalid cookie: Invalid cookie.
- invalid length: Invalid packet length.
- unknown exchange type: Unknown negotiation mode.
- uncritical drop: Unidentified non-critical payload.
- route limit: The number of injected routes has reached the upper limit.
- ip assigned fail: IP address allocation fails.
- local address mismatch: The local IP address in IKE negotiation and interface IP address do not match.
- dynamic peers number reaches limitation: The number of IKE peers reaches the upper limit.
- ipsec tunnel number reaches limitation: The number of IPsec tunnels reaches the upper limit.
- in disconnect state: The IPsec tunnel is torn down in disconnect state.
- netmask mismatch: The mask does not match the configured mask after the IPsec mask filtering function is enabled.
- flow conflict: A data flow conflict occurs.
- proposal mismatch or use sm in ikev2: IPsec proposals at both ends of the IPsec tunnel do not match or IKEv2 uses the SM algorithm.
- ikev2 not support sm in ipsec proposal ikev2: IKEv2 does not support the SM algorithm used in the IPsec proposal.
- no policy applied on interface: No policy is applied to an interface.
- none of user's interface is selected: Failed to select the tunnel interface in the user table based on the remote ID.
- nat detection fail: NAT detected failed.
- fragment packet limit: Fragment packets exceed the limit.
- fragment packet reassemble timeout: Fragment packet reassembly times out.

Procedure

- Cause: phase1 proposal mismatch
Check IKE proposal parameters at both ends of the IPsec tunnel and ensure that the parameters are consistent at both ends.

- Cause: phase2 proposal or pfs mismatch
Check IPsec proposal parameters or PFS algorithms at both ends of the IPsec tunnel and ensure that the parameters or algorithms are consistent at both ends.
- Cause: responder dh mismatch, initiator dh mismatch
Check DH algorithms at both ends of the IPsec tunnel and ensure that the algorithms are consistent at both ends.
- Cause: encapsulation mode mismatch
Check encapsulation modes at both ends of the IPsec tunnel and ensure that the encapsulation modes are consistent at both ends.
- Cause: eap authentication timeout, eap authentication fail, xauth authentication fail, xauth authentication timeout
Ensure that the client's user name and password as well as user access configuration are correct.
- Cause: ip assigned fail
Ensure that the AAA and IPsec configurations, such as the IP pool, AAA service scheme, and IP addresses assigned to IKE users, are correct.
- Cause: peer address mismatch
Check the IP addresses of IKE peers at both ends and ensure that the IP addresses match each other.
- Cause: config ID mismatch
Check identity authentication parameters, such as the ID type and ID value, and ensure that the parameters match each other.
- Cause: authentication fail
Check IKE proposal parameters or IKE peer parameters at both ends of the IPsec tunnel and ensure that the parameters are consistent at both ends.
- Cause: license or specification limited
Apply for a license or expand the capacity as required.
- Cause: exchange mode mismatch
Check the IKEv1 phase 1 negotiation modes at both ends and ensure that the negotiation modes are consistent at both ends.
- Cause: route limit
Replace the device with the one that has a higher route specification and plan the network properly.
- Cause: local address mismatch
Check the local IP address and interface IP address used in IKE negotiation and ensure that the IP addresses are consistent.
- Cause: ipsec tunnel number reaches limitation
Delete unnecessary IPsec tunnels or expand the capacity.
- Cause: dynamic peers number reaches limitation
Expand the capacity and plan the network properly.
- Cause: none of user's interface is selected
Check the ID type and ID value in the IKE user table as well as the interface associated with the IKE user, and ensure that these parameters match each other.

- Cause: in disconnect state
Check whether the link or device is working properly based on the IPsec link detection result.
- Cause: proposal mismatch or use sm in ikev2, ikev2 not support sm in ipsec proposal
Check the algorithm used by IKEv2 in the IPsec proposal and ensure that the algorithm is correct.
- Cause: flow conflict
Check ACL rules at both ends of the IPsec tunnel and ensure that the ACLs are correct.
- Cause: netmask mismatch
Change the IPsec-protected data flow range of the branch or headquarters to ensure that the data flow ranges negotiated by the branch and headquarters do not overlap.
- Cause: no policy applied on interface
Apply the required IPsec policy to the interface.
- Cause: fragment packet limit
The number of received fragmented packets exceeds the limit. Adjust the MTU of the peer device correctly.
- Cause: fragment packet reassemble timeout
Ensure that the links at both ends are normal and the device status is normal.
- If the fault persists, collect related information and contact technical support personnel.

3.1.49 ALM-4286193664 The SPR link status has changed

Description

SPR/4/SPRLINKCHANGE:OID [*oid*] SPR Link-state changed .LinkStateIndex = [*integer*], LinkStateName = [*octet*], LinkStateEligibility = [*integer*].

This alarm is generated when link quality parameters on a detection link become correct or incorrect.

Attribute

Alarm ID	OID	Alarm Severity	Alarm Type
4286193664	1.3.6.1.4.1.2011.5.25.241.2.2.1.1	Warning	Quality of service alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
LinkStateIndex	Indicates the index. The value ranges from 1 to 65535.
LinkStateName	Indicates the interface name.
LinkStateEligibility	Indicates the link status: • 0: indicates that the link is Up. • 1: indicates that the link is Down.

Impact on the System

- If a detection link reports this alarm when SPR is configured, the link may be unavailable.
- If a link sometimes reports this alarm, services may be switched normally.
- If a link frequently reports this alarm, link flapping occurs.

Possible Causes

1. Traffic is switched between links.
2. The link configuration is incorrect.
3. The threshold configuration is incorrect.
4. The link fails.

Procedure

1. Run the **display smart-policy-route link-state** command to view the detection link status.
 - Check whether the loss ratio is 1000. If yes, the link is faulty. Go to step 4.
 - Check whether the delay, jitter, loss ratio, and CMI are correct. If yes, go to step 2.
 - If the link status is not found, go to step 3.
2. Run the **display smart-service-profile service-map *name*** command to view thresholds for link quality parameters.
 - Check whether the link meets service requirements based on the link status. If link does not meet service requirements, services may be switched between links. Go to step 5.
 - Check whether the thresholds for link quality parameters are correct. If the thresholds for link quality parameters are incorrect, set correct thresholds for link quality parameters.
 - Run the **set delay threshold *threshold-value*** command to set the threshold for the delay.

- Run the **set jitter threshold** *threshold-value* command to set the threshold for the jitter.
- Run the **set loss threshold** *threshold-value* command to set the threshold for the loss ratio.
- Run the **set cmi threshold** *threshold-value* command to set the threshold for the CMI.
- Run the **cmi-method** *cmi-method* command to set the CMI formula.

Go to step 5.

3. Run the **display nqa results** [**test-instance** *admin-name test-name*] command to check whether the NQA test instance type is jitter.
 - If the NQA test instance type is jitter, the link is faulty. Go to step 4.
 - If the NQA test instance type is not jitter, reconfigure an NQA test instance and detection link. Go to step 5.
4. Collect the alarm information, log information, and configuration information, and then contact technical support personnel.
5. End.

3.1.50 ALM-4287373387 Temperature back to normal level

Description

ENTITYTRAP/4/ENTITYBRDTEMPRESUME:OID [OID] Temperature back to normal level.(Index=[INT1], EntryPhysicalIndex=[INT2], PhysicalName="[OCTET]",EntityThresholdType=[INT3],EntityThresholdValue=[INT4],EntityThresholdCurrent=[INT5], EntityTrapFaultID=[INT6])

This alarm is generated when the temperature of the entity is reduced to the allowed range.

Attribute

Alarm ID	OID	Alarm Severity	Alarm Type
4287373387	1.3.6.1.4.1.2011.5.25.219.2.10.14	Warning	environmentalAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
Index	Indicates the index of a temperature sensor.
EntryPhysicalIndex	Indicates the sub-index of an entity.

Name	Meaning
PhysicalName	Indicates the name of an entity.
EntityThresholdType 1: rise over 2: fall below	Indicates the alarm type.
EntityThresholdValue	Indicates the alarm threshold.
EntityThresholdCurrent	Indicates the current temperature.
EntityTrapFaultID	Indicates the cause ID of the alarm.

Impact on the System

None

Possible Causes

The temperature becomes within the range of the threshold.

Procedure

This alarm is a common notification and no action is required.

Related Information

None

3.1.51 ALM-4287373001 The Device ACL Resources Were Insufficient

Description

ENTITYTRAP/1/ACLRESOURCEEMPTY:OID [oid] The device acl resources were not enough.(Total=[INTEGER], Used=[INTEGER], Infomation=[STRING])

This is a major alarm, indicating that a traffic policy failed to be applied due to insufficient ACL resources.

Attribute

Alarm ID	OID	Alarm Severity	Alarm Type
4287373001	1.3.6.1.4.1.2011.5.1.2.3.3	Critical	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the ID of the alarm MIB object.
Total	Indicates the ACL specifications of the device.
Used	Indicates the number of ACLs in use.
Information	Indicates information about the traffic policy application failure.

Impact on the System

- The system does not support alarm clearance. You need to manually clear this alarm.
- The traffic policy failed to be applied due to insufficient ACL resources.

Possible Causes

- A traffic policy failed to be applied due to insufficient ACL resources.

Procedure

- Based on the alarm information, find the traffic policy that failed to be applied and the interface where the policy was to be applied.
- Delete an IPv4 or IPv6 ACL from the traffic policy and apply the policy again.
- If the fault persists, collect log information and configuration information, and then contact technical support personnel.

3.1.52 ALM-4287373002 The device acl resources were overloaded

Description

ENTITYTRAP/2/ACLRESOURCEOVERLOAD:OID [oid] The device acl resources were overloaded.(Total=[INTEGER], Used=[INTEGER], Usage=[INTEGER]%)

The ACL resource usage exceeded 90% of the threshold, and an ACL resource insufficiency alarm was generated.

Attribute

Alarm ID	OID	Alarm Severity	Alarm Type
4287373002	1.3.6.1.4.1.2011.5.1.2.3.1	Major	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the ID of the alarm MIB object.
Total	Indicates the ACL specifications of the device.
Used	Indicates the number of ACLs in use.
Usage	Indicates the current ACL resource usage.

Impact on the System

None

Possible Causes

The ACL resource usage exceeded 90%.

Procedure

- Each time an ACL is delivered, the system checks whether the ACL resource usage exceeds 90%. If so, the system generates an ACLresource insufficiency alarm.

3.1.53 ALM-303046881 The forwarding CPU usage exceeds the threshold

Description

ENTITYTRAP/2/CAPCPUUSAGERISING:OID [oid] Cap CPU utilization exceeded the pre-alarm threshold.(hwCapCPUThresholdType=[INTEGER], hwCapCPUThresholdCurrent=[INTEGER]%, hwCapCPUThresholdValue=[INTEGER]%)

The average CPU usage was too high during packet forwarding.

 NOTE

- If the average CPU usage is higher than 85% and lower than or equal to 95% during packet forwarding, this alarm is triggered for the first time. If the average CPU usage is higher than 95%, this alarm is triggered for the second time.
- For AR303, AR303W, AR611-S, AR611W-S, AR611E-S, AR611, AR631I-LTE4CN, AR631I-LTE4EA, AR611-LTE4EA, AR611W, AR611W-LTE4CN, AR611W-LTE6EA, AR617VW, AR617VW-LTE4, and AR617VW-LTE4EA. If the CPU usage is higher than 95%, this alarm is triggered.

Attribute

Alarm ID	OID	Alarm Severity	Alarm Type
303046881	1.3.6.1.4.1.2011.5.25.219.2.32.1	Major	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
hwCapCPUThresholdType	Indicates the average CPU usage threshold type during packet forwarding.
hwCapCPUThresholdCurrent	Indicates the current average CPU usage during packet forwarding.
hwCapCPUThresholdValue	Indicates the average CPU usage threshold during packet forwarding.

Impact on the System

Services are affected.

Possible Causes

The forwarded traffic volume was high.

Procedure

- Check whether the forwarded traffic volume is too high. If not, contact technical support personnel.

----End

3.1.54 ALM-303046882 The forwarding memory usage exceeds the threshold

Description

ENTITYTRAP/2/CAPMEMUSAGERISING:OID [oid] Cap Mem utilization exceeded the pre-alarm threshold.(hwCapMemType="[OCTET]", hwCapMemThresholdCurrent= [INTEGER]%, hwCapMemThresholdValue= [INTEGER]%)

The forwarding memory usage exceeds the alarm threshold.

Attribute

Alarm ID	OID	Alarm Severity	Alarm Type
303046882	1.3.6.1.4.1.2011.5.25.219.2.15.3	Major	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
hwCapMemType	Indicates the forwarding memory type.
hwCapMemThresholdCurrent	Indicates the current average forwarding memory usage.
hwCapMemThresholdValue	Indicates the average forwarding memory usage threshold.

Impact on the System

Services are affected.

Possible Causes

The average forwarding memory usage of the system is too high.

Procedure

- View information about tasks recorded with the forwarding memory usage in logs and contact technical support personnel.

----End

3.1.55 ALM-303046883 The forwarding single-core CPU usage exceeds the threshold

Description

ENTITYTRAP/2/CAPSINGLECORECPUUSAGERISING:OID [oid] Cap CPU utilization of single core exceeded the pre-alarm threshold.
(hwCapSingleCoreIndex=[INTEGER],
hwCapSingleCoreThresholdCurrent=[INTEGER]%,
hwCapSingleCoreThresholdValue=[INTEGER]%)

The CPU usage of a single forwarding core exceeds the alarm threshold.

Attribute

Alarm ID	OID	Alarm Severity	Alarm Type
303046883	1.3.6.1.4.1.2011.5.25.219.2.32.3	Major	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
hwCapSingleCoreIndex	Indicates the forwarding core ID.
hwCapSingleCoreThresholdCurrent	Indicates the CPU usage of the forwarding core.
hwCapSingleCoreThresholdValue	Indicates the CPU usage threshold of the forwarding core.

Impact on the System

Services are affected.

Possible Causes

The CPU usage of a single forwarding core in the system exceeds the alarm threshold.

Procedure

- View information about tasks recorded with the CPU usage of a single forwarding core in logs and contact technical support personnel.

----End

3.1.56 ALM-303046884 The device ESN has been changed

Description

ESN/4/ESNCHANGE:OID:[OID]The ESN has changed because the installation environment has changed.(OldESN=[OldESN], NewESN=[NewESN]).

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046884	Warning	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
OldESN	Original device ESN.
NewESN	New device ESN.

Impact on the System

The license becomes invalid since the device ESN is changed.

Possible Causes

The installation environment has been changed or the installation image is a copy.

Procedure

1. View the ESN change information in logs and contact technical support.
2. Apply for a new license using the new device ESN, and install and activate the license.

3.1.57 ALM-3224641536 The status of VRRP changed to master

Description

VRRP/2/VRRPCHANGETOMASTER:OID [OID] The status of VRRP changed to master. (VrrpIfIndex=[VrrpIfIndex], Vrid=[Vrid], IfIndex=[IfIndex], IPAddress=[Router-ID], NodeName=[NodeName], IfName=[IfName], ChangeReason=[ChangeReason])

The state of router changed to master.

Attribute

Alarm ID	OID	Alarm Severity	Alarm Type
3224641536	1.3.6.1.2.1.68.0.1	Major	environmentalAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
VrrpIfIndex	Index of the interface on which a VRRP backup group is configured
VrId	ID of a VRRP backup group
IfIndex	Index of the interface on which a VRRP backup group is configured
IPAddress	Router-ID of the device where a VRRP backup group is configured
NodeName	Device name
IfName	Name of the interface where a VRRP backup group is configured
ChangeReason	Cause for the change of the VRRP backup group status

Impact on the System

- If master/backup switchover occurs in normal cases, services are not affected.
- If master/backup switchover occurs in abnormal cases, services may be interrupted.

Possible Causes

Cause 1:

The former master router was faulty.

Cause 2:

The former master link was faulty.

Cause 3:

The priority of the former master router or backup router changed.

Cause 4:

The logical interface where the VRRP backup group resides on the master router is deleted or the configuration of the VRRP backup group is deleted.

Cause 5:

The former master router recovers from a fault.

Cause 6:

The former master link recovers from a fault.

Procedure

- Step 1** View user logs to check the causes of the VRRP change. You can perform operations according to the specific cause.
- If the cause is priority calculation, go to step 6.
 - If the cause is that the MASTER_DOWN timer expired, go to step 2.
 - If the cause is the change of the BFD session status, go to step 2.
 - If the cause is the change of the interface status, go to step 2.
 - If the cause is admin-vrrp DROVE, go to step 6.
- Step 2** Run the **display vrrp** command to check the status of the VRRP backup group on the former master router.
- If the VRRP backup group is in the Initialize state, the former router is faulty. Locate the cause of the fault and restore the master router. Go to step 6.
 - If the VRRP backup group is in the Backup state, go to step 6.
 - If the VRRP backup group is in the Master state, go to step 3.
- Step 3** Check whether the master link is faulty.
- If BFD is configured, go to step 4.
 - If BFD is not configured, go to step 5.
- Step 4** Run the **display vrrp** command to check the status of the BFD session.
- If the BFD session is Down, it indicates that the former master link is faulty. Locate the cause of the fault and restore the master link. Go to step 8.
 - If the BFD session is Up, go to step 7.
- Step 5** Run the **display vrrp [interface *interface-type interface-number*] [virtual-router-id] statistics** command to check whether the VRRP packets are normally forwarded.
- If not, it indicates that the link is faulty. Locate the cause of the fault and restore the link. Go to step 8.
 - If so, go to step 7.
- Step 6** On the former master router and backup router, run the **display vrrp** command to check whether the configured priority of the VRRP is consistent with the running priority.
- If not, it indicates that the link monitored through VRRP is faulty. Locate the cause of the fault and restore the monitored link. Go to step 8.

- If so, go to step 7.

Step 7 Collect alarm information and configuration information, and then contact technical support personnel.

Step 8 End.

----End

Clearing

After the fault is rectified, the system clears this alarm, removing the need to manually clear it. This alarm will not be displayed on the **Current Alarms** page.

3.1.58 ALM-3224641538 The state of VRRP changed from master to other state

Description

VRRP/2/VRRPMASTERDOWN:OID [OID] The state of VRRP changed from master to other state. (VrrplfIndex=[VrrplfIndex], Vrid=[Vrid], IfIndex=[IfIndex], IPAddress=[IPAddress], NodeName=[NodeName], IfName=[IfName], CurrentState=[CurrentState], ChangeReason=[ChangeReason])

The VRRP backup group was changed from the Master state to another state.

Attribute

Alarm ID	OID	Alarm Severity	Alarm Type
3224641538	1.3.6.1.4.1.201.1.5.25.127.2.3.0.1	Major	Communication alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
VrrplfIndex	Index of the interface on which a VRRP backup group is configured
Vrid	ID of a VRRP backup group

Name	Meaning
IfIndex	Index of the interface on which a VRRP backup group is configured
IpAddress	Router ID of the device
NodeName	Device name
IfName	Name of the interface where a VRRP backup group is configured
CurrentState	VRRP backup group status after the change: • Notactive: Indicates that the VRRP backup group in the master state is deleted. Configurations of this VRRP backup group cannot be viewed by using the display vrrp command. • Initialize • Backup
ChangeReason	Cause for the change of the VRRP backup group status

Impact on the System

- If master/backup switchover occurs normally, services are not affected.
- If master/backup switchover occurs abnormally, services may be interrupted.

Possible Causes

Cause 1:

The master router was faulty.

Cause 2:

The active link was faulty.

Cause 3:

The priority of the VRRP backup group on the master router or the slave router changed.

Cause 4:

The logical interface where the VRRP backup group resides on the master router is deleted or the configuration of the VRRP backup group is deleted.

Cause 5:

The former master router recovers from a fault.

Cause 6:

The former active link recovers from a fault.

Procedure

- Step 1** View the value of CurentState in the alarm, check the status after the VRRP backup group changes, and perform operations according to the specific cause.
- If the value of CurentState is Notactive, go to step 2.
 - If the value of CurentState is Backup, go to step 3.
 - If the value of CurentState is Initialize, go to step 4.
- Step 2** If the VRRP backup group in the Master state is deleted, you cannot view the configurations of the VRRP backup group by using the **display vrrp** command. You can check the operation records of command lines by viewing log information.
- Step 3** Run the **display vrrp** command to check whether the set priorities of the VRRP backup group on the original master router and backup router are the same as the running priorities.
- If so, go to step 7.
 - If not, it indicates that the link monitored by the VRRP backup group is faulty and the priorities are increased or reduced. Locate the cause of the fault and restore the monitored link. Then, go to step 4.
- Step 4** If the original master router is faulty, locate the cause of the fault and restore the master router.
- Check whether the interface where the VRRP backup group resides is normal, and then go to step 6.
 - Check whether the link that the VRRP backup group monitors is normal, and then go to step 7.
 - If the VRRP backup group and BFD are associated, check the link that BFD monitors and go to step 5.
- Step 5** Run the **display vrrp** command to check the status of the BFD session.
- If the BFD session is Up, go to step 8.
 - If the BFD session is Down, it indicates that the original active link is faulty. Locate the cause of the fault and restore the active link. Then, go to step 9.
- Step 6** Run the **display vrrp [interface *interface-type interface-number*] [virtual-router-id] statistics** command to check whether VRRP Advertisement packets can be normally received and sent.
- If so, go to step 8.
 - If not, it indicates that the link is faulty. Locate the cause of the fault and restore the link. Then, go to step 9.
- Step 7** Run the **display vrrp** command to view the interface that is monitored by the BFD session associated with the VRRP backup groups and then enter the interface view to run the **display this interface** command to detect the interface status.
- If the interface status is Up, go to step 8.
 - If the interface status is Down, it indicates that the link is faulty. Locate the cause of the fault and restore the active link. Then, go to step 9.
- Step 8** Collect alarm information and configuration information, and then contact technical support personnel.

Step 9 End.
----End

Clearing

After the fault is rectified, the system clears this alarm, removing the need to manually clear it. This alarm will not be displayed on the **Current Alarms** page.

3.1.59 ALM-3488620546 Interface Monitor Input Rate Rising

Description

IFNET/4/INBWRATEEXCEED: OID [OID] Interface input flow bandwidth usage exceeded the trap threshold. (Interface=[INTEGER], BandWidthUsage=[INTEGER], TrapThreshold=[INTEGER], InterfaceName=[STRING])

The trap was generated when the percentage of the rate of received traffic to the total bandwidth on an interface was greater than the threshold.

Attribute

Alarm ID	OID	Alarm Severity	Alarm Type
3488620546	1.3.6.1.4.1.201.1.5.25.41.4.5	Major	other

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
Interface	Indicates the interface index.
BandWidthUsage	Indicates bandwidth usage.
TrapThreshold	Indicates the trap threshold of bandwidth usage.
InterfaceName	Indicates the interface name.

Impact on the System

When the rate of traffic is close to 100% out of the total bandwidth, delay or packet loss will occur.

When traffic rate is approximate to the maximum interface bandwidth, service packets may be dropped.

Possible Causes

The rate of traffic received by the interface was too large.

Procedure

Step 1 Run the **display this interface** command on the interface to check whether the traffic threshold is too low. The threshold range is specified by users according to actual services.

- If so, go to Step 2.
- If not, go to Step 3.

Step 2 Run the **trap-threshold input-rate** *threshold_value* command to reset the threshold and then check whether the alarm is cleared.

- If so, go to Step 7.
- If not, go to Step 3.

Step 3 Run the **display this interface** command in the interface view to check the number and types of packets on the interface. Determine whether the packet sending and receiving is abnormal due to a failure such as loop.

- If so, go to Step 4.
- If not, go to Step 5.

Step 4 Find out the abnormal packets and eliminate the impact of abnormal packets. Check whether the alarm is cleared.

- If so, go to Step 7.
- If not, go to Step 5.

Step 5 Expand capacity in any of the following ways:

- Configure an Eth-Trunk to load balance traffic.
- Migrate some services to idle devices.
- Use the link with higher bandwidth to transmit service packets.

After the operation, check whether the alarm is cleared.

- If so, go to Step 7.
- If not, go to Step 6.

Step 6 Collect trap messages, log messages, and configurations, and then contact the technical support personnel.

Step 7 End.

----End

Clearing

After the certificate is deleted, the system clears this alarm, removing the need to manually clear it. This alarm will not be displayed on the **Current Alarms** page.

3.1.60 ALM-4285603840 NAT Packet Discard

Description

NAT/4/NAT_PACKET_DISCARD: OID [OID] Interface [OCTET] had discarded packets, due to lack of mapping space when NAT is out of addresses.

The NAT address pool resources are insufficient. As a result, NAT packet loss event alarm is displayed when packet loss occurs.

Attribute

Alarm ID	OID	Alarm Severity	Alarm Type
428560Processing error alarm3840	1.3.6.1.4.1.201.1.5.25.123.2.6	Minor	Processing error alarm

Parameters

Name	Meaning
OID	MIB object number
OCTET	Interface index

Impact on the System

None

Possible Causes

Packet loss occurs because of insufficient NAT address pool resources of the interface index.

Procedure

This is a normal notification.

The alarm is generated when the IP addresses referenced by outbound NAT (no-PAT) are insufficient for outbound NAT configuration.

Clearing

The alarm needs to be cleared manually.

3.1.61 ALM-3245219843 Ethernet ARP IP Conflict Event

Description

ARP/4/ARP_IPCONFLICT_TRAP:OID [OID] ARP detects IP conflict. (IP address=[IPADDR], Local interface=[OCTET], Local MAC=[OCTET], Local vlan=[INTEGER], Local CE vlan=[INTEGER], Receive interface=[OCTET], Receive MAC=[OCTET], Receive vlan=[INTEGER], Receive CE vlan=[INTEGER], IP conflict type=[OCTET]).

An IP address conflict is detected by ARP.

Attribute

Alarm ID	OID	Alarm Severity	Alarm Type
3245219843	1.3.6.1.4.1.201.1.5.25.123.2.6	Major	environmentalAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
IP address	IP address.
Local interface	Interface recorded in the ARP entry of the IP address.
Local MAC	Source MAC address recorded in the ARP entry of the IP address.
Local vlan	VLAN recorded in the ARP entry of the IP address.

Name	Meaning
Local CE vlan	CEVLAN recorded in the ARP entry of the IP address.
Receive interface	Inbound interface of the second ARP packet with the IP address.
Receive MAC	Source MAC address of the second ARP packet with the IP address.
Receive vlan	VLAN configured on the inbound interface of the second ARP packet with the IP address.
Receive CE vlan	CEVLAN configured on the inbound interface of the second ARP packet with the IP address.
IP conflict type	IP address conflict type.

Impact on the System

This alarm indicates that an IP address conflict occurred. If the IP address conflict is not eliminated timely, route flapping may occur and services may be interrupted.

Possible Causes

- Cause 1: The source IP address in an ARP packet is the same as the IP address of the inbound interface that receives the ARP packet, but the source MAC address in the ARP packet is different than the MAC address of the inbound interface.
- Cause 2: The source IP address in an ARP packet is the same as the IP address in an existing ARP entry, but the source MAC address is different than the MAC address in the ARP entry.
- Cause 3: The source IP address in an ARP packet is 0.0.0.0 (probe ARP packet), the destination IP address is the same as the IP address of the inbound interface that receives the ARP packet, but the source MAC address in the ARP packet is different than the MAC address of the inbound interface.

Procedure

Step 1 Identify the devices or users who use the same IP address.

- If the devices or users using the same IP address can be identified, modify the IP address of one device or user. Then, go to step 2.
- If the devices or users using the same IP address cannot be identified. Collect alarm information and configuration information, and then contact technical support personnel.

Step 2 End.

----End

Clearing

The alarm needs to be cleared manually.

3.1.62 ALM-3224903681 User Login

Description

LINE/5/USERLOGIN: OID [OID] A user login. (UserIndex=[INTEGER], UserName=[STRING], UserIP=[STRING], UserChannel=[STRING])

This alarm is generated when a user logs in to the device.

Attribute

Alarm ID	OID	Alarm Severity	Alarm Type
3224903681	1.3.6.1.4.1.201.1.5.25.207.2.2	Warning	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
UserIndex	Indicates the index of a user.
UserName	Indicates the name of a user.
UserIP	Indicates the IP address of a user.
UserChannel	Indicates the channel used by a user.

Impact on the System

None

Possible Causes

A user logged in to the device.

Procedure

This alarm is informational and no action is required.

Clearing

The alarm needs to be cleared manually.

3.1.63 ALM-3224903682 User Login Fail

Description

LINE/4/USERLOGINFAIL:OID [OID] A user login fail. (UserIndex=[INTEGER], UserName=[STRING], UserIP=[STRING], UserChannel=[STRING])

A user failed to log in to the device.

Attribute

Alarm ID	OID	Alarm Severity	Alarm Type
3224903682	1.3.6.1.4.1.201.1.5.25.207.2.3	Warning	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
UserIndex	Index of a user.
UserName	Name of a user.
UserIP	IP address of a user.
UserChannel	Channel for login.

Impact on the System

None

Possible Causes

A user failed to log in to the device.

Procedure

Check whether the user password is correct.

- If the user password is correct, contact technical support personnel.
- If the user password is incorrect, log in to the device again using the correct password.

Clearing

The alarm needs to be cleared manually.

3.1.64 ALM-3224903683 User Logout

Description

LINE/5/USERLOGOUT: OID [OID] A user logout. (UserIndex=[INTEGER], UserName=[STRING], UserIP=[STRING], UserChannel=[STRING])

This alarm is generated when a user logs out to the device.

Attribute

Alarm ID	OID	Alarm Severity	Alarm Type
3224903683	1.3.6.1.4.1.201.1.5.25.207.2.4	Warning	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
UserIndex	Indicates the index of a user.
UserName	Indicates the name of a user.
UserIP	Indicates the IP address of a user.

Name	Meaning
UserChannel	Indicates the channel used by a user.

Impact on the System

None

Possible Causes

A user logged out to the device.

Procedure

This alarm is informational and no action is required.

Clearing

The alarm needs to be cleared manually.

3.1.65 ALM-4286193665 The Current Link of the SPR Service Profile Changed

Description

SPR/4/SERVICEMAP_LINKCHANGE:OID [*OID*] SPR Service-map Link changed.
ServiceIndex = [*integer*], ServiceName = [*octet*], ServiceCurLinkName = [*octet*],
System Name = [*string*], Original Ip address = [*string*].

The current link of the SPR service profile changed.

Attribute

Alarm ID	Alarm Severity	Alarm Type
4286193665	Major	Quality of service alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
ServiceIndex	Indicates an entry index. The value ranges from 1 to 65535.
ServiceName	Indicates the name of a service profile.

Name	Meaning
ServiceCurLinkName	Indicates the current link name of the service profile.
System Name	Indicates the system name.
Original Ip address	Indicates the link IP address used before link switching.

Impact on the System

- If the SPR service profile has just been configured, it is normal that this alarm is sent. This will not affect the system.
- If the alarm of a service profile is sent occasionally, normal link switching may have occurred. This will not affect the system.
- If the alarm of a service profile is sent frequently, the link to which the service profile is bound may flap.

Possible Causes

1. The service threshold configuration is incorrect.
2. The link to which the service profile is bound is faulty.

Procedure

Step 1 Check the SPR status.

Log in to the iMaster NCE-Campus as a tenant administrator. Choose **Maintenance > Provisioning Result > Site Configuration Status** from the main menu.

On the **Configuration Result** tab page, click  next to a device, click **Intelligent policy-based routing** on the **Feature List** tab page, and click **For Details** to view the SPR status of the corresponding device.

- If the link status is normal, no operation is required.
- If not, modify the SPR parameters.

Step 2 Check the traffic switchover thresholds.

Log in to the iMaster NCE-Campus as a tenant administrator. Choose **Policy > WAN Policy > Traffic Policy** from the main menu, click the **Intelligent Traffic Steering** tab under **Overlay**. On the tab page that is displayed, check the traffic switchover thresholds set in the traffic policy configured for the faulty device.

- If the settings are correct, no operation is required.
- If not, select the policy and click the modification icon in the **Operation** column. Then, enable **Advanced settings**, and set **Switch upper threshold** and **Switch lower threshold**.

Step 3 Check the quality of the links bound to the SPR service profile.

Log in to the iMaster NCE-Campus as a tenant administrator. Choose **Maintenance > Diagnosis > Ping** from the main menu. In the **Results** area, check the link status of the corresponding device.

- If the link status is normal, no operation is required.
- If not, run the **display smart-policy-route dest-site all** command on the faulty device to check the link quality.
Check whether the values of loss, delay, and jitter exceed the thresholds on the iMaster NCE-Campus web UI. If the value of any parameter exceeds the threshold, services are switched between links.

Step 4 Collect alarm information, log information, and configuration, and contact technical support personnel.

Step 5 End.

----End

Clearing

The alarm needs to be cleared manually.

3.1.66 ALM-1880563712 The status of the OSPF interface was down

Description

OSPF/2/IFCHG:OID [OID]: The status of the non-virtual interface changes. (IfIpAddress=[ipaddr], AddressLessIf=[integer], ProcessId=[integer], AreaId=[ipaddr], IfnetIndex=[integer], ProcessId=[integer], RouterId=[ipaddr], IfState=[integer], IfName=[octet], InstanceName=[octet], IfChgReason=[integer])

The status of the OSPF non-virtual-link interface changed. The possible cause was that the physical interface was Down.

Attribute

Alarm ID	OID	Alarm Severity	Alarm Type
1880563712	1.3.6.1.2.1.14.16.2.1.6	Major	environmentalAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
IfIpAddress	Indicates the IP address of the non-virtual-link interface.
AddressLessIf	Indicates the index of the interface.
ProcessId	Indicates the process ID.
AreaId	Indicates the area ID.
IfnetIndex	Indicates the Ifnet index of the interface.
ProcessId	Indicates the process ID.
RouterId	Indicates the router ID of the local router.
IfState	Indicates the status of the interface. 1: Down 2: Loopback 3: Waiting 4: Point-to-Point 5: DR 6: Backup 7: DROther
IfName	Indicates the name of interface.
InstanceName	Indicates the instance name.

Name	Meaning
IfChgReason	Indicates the reason why the neighbor status changes: • 1 (adjacencyHoldTimerExpired): indicates that the timer of the adjacent router times out. • 2 (physicalInterfaceChange): indicates that the status of the physical interface on the router changes. • 3 (ospfProtocolReason): indicates that an alarm is generated because of the OSPF protocol. • 4 (bfdSessionStateChange): indicates that the BFD session is closed. • 5 (configureChange): indicates that the OSPF configuration changes. • 6 (peerRouterReason): indicates that an alarm is generated because of the neighboring router. • 100 (alarmCleared): indicates that the alarm is cleared because services are restored or the neighbor is deleted.

Impact on the System

If the interface status becomes Down, services may be affected. If the interface status becomes DR, BDR, DRoother, or P2P, services will not be affected.

Possible Causes

1. The status of the physical interface changed.
2. DR election occurred on the broadcast network.

Procedure

- Step 1** Run the **display ospf interface** command to check whether the interface is Down.
- If the interface is Down, go to step 2.
 - If the interface is in another state, services are not affected. Then, go to step 4.
- Step 2** Run the **display interface *interface-type* *interface-number*** command to check whether the current interface is Up.
- If so, go to step 3.

- If not, view the log file to check whether the **shutdown** command is run on the interface.
 - If the **shutdown** command is run on the interface, in the case of an incorrect operation, run the **undo shutdown** command on the interface; otherwise, go to step 4.
 - If the **shutdown** command is not run on the interface, it indicates that the link is faulty. Thus, replace the link or go to step 3.

Step 3 Collect alarm information and configuration information, and then contact technical support personnel.

Step 4 End.

----End

Clearing

After the fault is rectified, the system clears this alarm, removing the need to manually clear it. This alarm will not be displayed on the **Current Alarms** page.

3.1.67 ALM-4289404934 All connections between sites have entered down state

Description

CONN/4/CONN_SITE_DISCONNECT:OID [oid] All connections between sites have entered down state. (SrcSite=[integer1], DestSite=[integer2])

SD-WAN EVPN sites are disconnected.

Attribute

Alarm ID	OID	Alarm Severity	Alarm Type
4289404934	1.3.6.1.4.1.20 11.5.25.241. 6.3.8	Major	Communication alarm

Parameters

Name	Meaning
oid	Indicates the MIB object ID of the alarm.
SrcSite	Name of the source site.
DestSite	Name of the destination site.

Impact on the System

All EVPN links between sites are in the Down state.

For each EVPN link in the Down state, the possible causes are as follows:

- No keepalive packet is received from the peer device within the configured detection period.
- A change in the protocol status of a physical interface may cause a change in the link status.
- The BGP protocol established with the remote site is interrupted.

Possible Causes

- Cause 1: KA detection fails.
- Cause 2: The KA status is abnormal.
- Cause 3: The interface went Down.
- Cause 4: The interface address was changed.
- Cause 5: NAT probe failed.
- Cause 6: BGP instructs the TNP to be deleted.
- Cause 7: BGP instructs the TNP to be updated.
- Cause 8: The TNP weight changes.
- Cause 9: The TNP configuration is changed.
- Cause 10: DTLS notification.
- Cause 11: The user is reset.
- Cause 12: The diagnosis is complete.
- Cause 13: The service route of the site was deleted.
- Cause 14: The DH group does not match.
- Cause 15: The DH group changes.
- Cause 16: Self-healing was recovered.
- Cause 17: The dynamic tunnel was aged.
- Cause 18: The dynamic tunnel was blocked.
- Cause 19: The dynamic tunnel was cleared.
- Cause 20: Other causes.

Procedure

1. Check whether the interfaces bound to the TNP can be pinged.
 - If yes, go to Step 23.
 - If not, go to step 2.
2. Check whether the intermediate transmission network is faulty.
3. The inspection method is the same as that in step 1 and step 2.
4. Check whether the physical protocol status of the interface bound to the TNP is Up.
5. Check whether the **shutdown** command is run on the interface.

6. Check whether the IP address of the interface bound to the TNP is changed.
7. Check whether the interfaces bound to the TNP can be pinged.
 - If yes, go to Step 23.
 - If not, go to step 8.
8. Check whether ports 3478 and 4500 are restricted on the intermediate transport network.
9. Run the **display site-tnp site-id** command to check whether the TNP of the peer device is deleted.
 - If yes, configure the TNP information.
 - If no, collect alarm and configuration information and contact technical support.
10. Check whether the service route to the corresponding site changes.
11. Run the **display site-tnp site-id verbose** command to check whether the TNP weight changes.
12. Run the **display site-tnp site-id verbose** command to check whether the TNP bandwidth changes.
13. Check whether the ESN blocklist and trustlist function is configured.
14. Check whether BGP or connection reset is performed on the local device.
15. Check whether the device has flapped.
16. Check whether the service route to the corresponding site is deleted.
 - a. Run the **display tunnel all** command to view information about all tunnels.
 - b. Run the **display tunnel tunnel-id** command to check information about SD-WAN tunnels one by one and check whether service routes exist.
 - If it does not exist, configure the corresponding site route.
 - If yes, collect alarm and configuration information and contact technical support.
17. Check whether the DH group of the local device matches that of the peer device.

Run the **display ipsec p2mp-policy** command to check information about IPsec Key Exchange on both ends. If the DH groups of the two communication parties are different and one party uses the strict mode, the DH groups cannot be matched. Configure the same DH group or disable the strict mode.
18. Run the **display ipsec p2mp-policy** command to check key-exchange information on the peer device. Check whether the DH group is changed.
19. The device detects that the connection is abnormal and recovers from self-healing.
20. Run the **display smart-policy-route** command to check whether dynamic tunnels are enabled. If dynamic tunnels are enabled, check whether traffic does not exist.
 - If the traffic persists, go to Step 23.
 - If the traffic is not present, it is normal.

21. Run the **display smart-policy-route** command to check whether dynamic tunnels are enabled. If dynamic tunnels are enabled, check whether the number of links exceeds the upper limit.
 - If the number exceeds the specifications, the RR/HUB site resources are insufficient.
 - If the number does not exceed the specifications, collect alarm and configuration information and contact technical support.
22. Run the **display smart-policy-route** command to check whether dynamic tunnels are enabled.
 - If dynamic tunnels are enabled, unnecessary links are cleared.
 - If not, collect alarm and configuration information and contact technical support.
23. Collect alarm and configuration information and contact technical support.

Clearing

After the fault is rectified, the system clears this alarm, removing the need to manually clear it. This alarm will not be displayed on the **Current Alarms** page.

3.1.68 ALM-4289601651 The number of forward sessions has reached the threshold value

Description

FWDTRAP/2/SESSIONRESLACKREPORT: OID [oid] The forward session resources were overloaded.(SessionType = "[OCTET]", ThresholdLevel = [INTEGER], CurrentNum = [INTEGER], TotalNum = [INTEGER], Usage = [INTEGER]%, Top3SourceIpAddress=[OCTET])

The number of forwarding flow tables on the device reaches or exceeds 90% or 100% of the maximum number, an alarm is generated.

NOTE

- If the number of forwarding flow tables changes too rapidly within a short period of time, multiple alarms may be generated. As a result, the system records these alarms, affecting normal services on the device. To prevent the device from recording a large number of alarms, the system suppresses the alarms by setting the interval at which alarms are sent to longer than 30 minutes. That is, the system records an alarm at least 30 minutes after the last alarm was cleared.
- This alarm is supported in V300R022C00SPC100 and later versions.

Attribute

Alarm ID	OID	Alarm Severity	Alarm Type
4289601651	1.3.6.1.4.1.20 11.5.25.227. 2.1.38	Major	Quality Of Service Alarm

Parameters

Name	Meaning
[oid]	Indicates the MIB object ID of the alarm.
SessionType	Alarm type. Currently, only SESSION is supported.
ThresholdLevel	Alarm severity: 1: indicates level-1 alarms. The alarm threshold is 90%. 2: indicates level-2 alarms. The alarm threshold is 100%.
CurrentNum	Number of forwarding flow tables.
TotalNum	Maximum number of forwarding flow tables.
Usage	Proportion that the number of forwarding flow tables on the device accounts for of the maximum number.
Top3SourceIpAddress	Three source IP addresses with the largest number of forwarding flow tables and their corresponding numbers of forwarding flow tables. Format: (<i>Source IP address 1, Number of forwarding flow tables 1</i>) (<i>Source IP address 2, Number of forwarding flow tables 2</i>) (<i>Source IP address 3, Number of forwarding flow tables 3</i>)

Impact on the System

Services are affected.

Possible Causes

- Cause 1: The number of forwarding flow tables on the device reached or exceeded the level-1 alarm threshold (90%).
- Cause 2: The number of forwarding flow tables on the device reached or exceeded the level-2 alarm threshold (100%).

Procedure

Check service configurations and contact technical support personnel.

Clearing

After the fault is rectified, the system clears this alarm, removing the need to manually clear it. This alarm will not be displayed on the **CurrentAlarms** page.

3.1.69 ALM-4289601647 The backup link is in use

Description

CONN/4/CONN_BACKUP_LINK_IN_USE_TRAP:OID [oid]The backup link is in use.
(InterfaceName=[STRING])

The backup link is in use.

Attribute

Alarm ID	OID	Alarm Severity	Alarm Type
4289601647	1.3.6.1.4.1.20 11.5.25.241. 6.3.8	Major	Communication alarm

Parameters

Name	Meaning
oid	Indicates the MIB object ID of the alarm.
InterfaceName	Indicates the interface name.

Impact on the System

If the standby link is used, services may be interrupted or a large amount of wireless traffic may be used.

Possible Causes

The master link is faulty.

Procedure

Restore the primary link. If the active link is normal, collect alarm information and configuration information, and contact technical support.

Clearing

After the fault is rectified, the system clears this alarm, removing the need to manually clear it. This alarm will not be displayed on the **Current Alarms** page.

3.1.70 ALM-4289601648 RDB file recovery

Description

CFMY/4/CFMY_RDB_RECOVERY: OID [oid] The RDB is recovery, the possible cause is that the device is powered off or the flash is damaged.

The RDB is recovery, the possible cause is that the device is powered off or the flash is damaged.

Attribute

Alarm ID	OID	Alarm Severity	Alarm Type
4289601648	1.3.6.1.4.1.20 11.5.25.19.2. 41	Minor	Communication alarm

Parameters

Name	Meaning
oid	Indicates the MIB object ID of the alarm.

Impact on the System

The configurations delivered last time from the controller cannot be restored.

Possible Causes

The RDB file may be damaged due to power failure or the flash memory may be damaged.

Procedure

1. Run the **display reset-reason [slotslot-id]** command to check the reset cause.
2. Check whether the flash memory of the device is damaged.

Clearing

After the fault is rectified, the system clears this alarm, removing the need to manually clear it. This alarm will not be displayed on the **Current Alarms** page.

3.1.71 ALM-4289601650 The number of connections has reached the threshold value

Description

ARP/4/ARP_THRESHOLD_EXCEED_TRAP:OID [OID] The number of ARP entries exceeded the threshold. (entPhysicalIndex=[INTEGER], Slot name=[OCTET], Threshold=[COUNTER], Number of dynamic ARP entries=[COUNTER], Number of static ARP entries=[COUNTER]).

The number of ARP entries exceeds the upper threshold.

Attribute

Alarm ID	OID	Alarm Severity	Alarm Type
4289601650	1.3.6.1.4.1.2011.5.25.123.2.4	Major	Quality Of Service Alarm

Parameters

Name	Meaning
oid	Indicates the MIB object ID of the alarm.
entPhysicalIndex	Indicates the index of the physical entity.
Slot name	Indicates the board LPU device name.
Threshold	Indicates the alarm threshold, that is, 80 percent of the total number of ARP entries supported by the switch. The alarm threshold cannot be modified.
Number of dynamic ARP entries	Indicates the number of dynamic ARP entries.
Number of static ARP entries	Indicates the number of static ARP entries.

Impact on the System

If this alarm is displayed, the number of ARP entries on the device is great. If the number continuously increases, system resources become insufficient and no new ARP entries can be learned. As a result, service interruption may occur.

Possible Causes

The number of ARP entries on the device exceeded the upper threshold.

Procedure

1. Run the **display arp statistics all** command to view ARP entry statistics on the device and check whether there are more static ARP entries or dynamic ARP entries.
 - If there are more dynamic ARP entries, go to Step 2.
 - If there are more static ARP entries, go to Step 3.
2. Run the **display arp all** command to identify the interface that has more ARP entries. Then run the **display arp interface** command to check ARP entries on the interface and determine whether these ARP entries are necessary for the interface.
 - If these ARP entries are necessary, go to Step 5.
 - If these ARP entries are not necessary, run the **reset arp** command to delete certain ARP entries (without system running being affected) and go to Step 4.
3. Run the **display current-configuration** command to view static ARP entries and check whether these static ARP entries are necessary.
 - If these static ARP entries are necessary, go to Step 5.
 - If these static ARP entries are not necessary, run the **undo arp static** command to delete certain static ARP entries (without system running being affected) or run the **reset arp static** command to clear all static ARP entries. Then go to Step 4.
4. Run the **display arp statistics all** command to check whether the number of ARP entries still continuously increases unexpectedly.
 - If the number of ARP entries does not continuously increase, go to Step 6.
 - If the number of ARP entries still continuously increases, go to Step 5.
5. Collect alarm information and configuration information, and then contact Huawei technical support personnel..
6. End.

Clearing

After the fault is rectified, the system clears this alarm, removing the need to manually clear it. This alarm will not be displayed on the **Current Alarms** page.

3.1.72 ALM-135471746 hwDeviceFaultAlarm

Description

The device is faulty. (PhysicalID=[PhysicalId],PhysicalName=[PhysicalName])

Attribute

Alarm ID	OID	Alarm Severity	Alarm Type
135471746	1.3.6.1.4.1.20 11.5.25.123. 2.4	Critical	Equipment Alarm

Parameters

Name	Meaning
PhysicalID	Indicates the ID of the Physical.
PhysicalName	Indicates the name of the Physical.

Impact on the System

Services on the device are abnormal.

Possible Causes

- Cause 1: The peripheral components are abnormal.
- Cause 2: The PHY is abnormal.
- Cause 3: The IIC is abnormal.

Procedure

Collect alarm information and configuration information, and then contact Huawei technical support personnel.

Clearing

After the fault is rectified, the system clears this alarm, removing the need to manually clear it. This alarm will not be displayed on the **Current Alarms** page.

3.2 V500 Firewall Alarms

3.2.1 ALM-303046708 CPU usage exceeds the threshold

Description

ENTEXT/4/CPUUSAGE:[*OID*] Entity [*index*]: The [*cpu_name*] CPU is overload. ([*current-cpu-usage*] > [*cpu-usage-threshold*]).

The CPU usage exceeded the threshold.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046708	Warning	environmentalAlarm

Parameters

Name	Meaning
<i>OID</i>	Indicates the MIB node ID.
<i>index</i>	Indicates the CPU index.
<i>cpu_name</i>	Indicates the name of a CPU for the device, management plane, or data plane.
<i>current-cpu-usage</i>	Indicates the current CPU usage.
<i>cpu-usage-threshold</i>	Indicates the CPU usage threshold. The default value is 80% and can be changed.

Impact on the System

When the CPU usage is high, the processing of protocol packets is affected.

Possible Causes

The current CPU usage is too high.

Procedure

Check the services and configurations enabled on the device. If the CPU usage keeps high, contact the technical support personnel.

Clearing

Event alarm: indicates that a system event occurs and the alarm does not need clearing.

Related Information

None

3.2.2 ALM-303046707 Memory usage exceeds the threshold

Description

ENTEXT/4/MEMORYUSAGE:[OID] Entity [index]: The entity memory is overload([current-memory-usage] > [memory-usage-threshold], MemoryTotalSize=[memory-total]KB).

The memory usage exceeded the threshold.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046707	Warning	environmentalAlarm

Parameters

Name	Meaning
OID	Indicates the MIB node ID.
index	Indicates the index of memory in the system. • 0: malloc • 1: vrp vos_malloc • 2: vrpio vos_malloc • 3: sos_malloc
current-memory-usage	Indicates current memory usage.
memory-usage-threshold	Indicates the memory usage threshold. The default value is interface memory threshold and can be changed.
memory-total	Indicates the total memory.

Impact on the System

The device performance deteriorates. If the memory usage continues to increase, the device will restart for protection.

Possible Causes

The current memory usage is too high.

Procedure

Contact the technical personnel.

Clearing

Event alarm: indicates that a system event occurs and the alarm does not need clearing.

Related Information

None

3.2.3 ALM-303046710 A card has stopped working

3.2.3.1 ALM-303046710 A card has stopped working 132626

Description

SRM_ENTITY/1/BOARDINVALID: OID 1.3.6.1.4.1.2011.5.25.219.2.2.5 The board totally failed. (EntityPhysicalIndex=[integer], EntityPhysicalIndex=[integer], EntPhysicalName="[STRING]", EntityType=[integer], EntityTrapFaultID=132626)
 The board experienced a complete failure.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046710	Critical	equipmentAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
EntityPhysicalIndex	Indicates the index of the physical entity.
EntityPhysicalIndex	Indicates the index of the physical entity.
EntPhysicalName	Indicates the name of the physical entity, such as "SFU LPU MPU slot <slotID>". The entity name varies according to the board type, such as the SFU, LPU, and MPU.
EntityType	Indicates the type of the entity, such as mpu(1), lpu(2), sfu(3), pic(4), cfc card(5), and ofc(6).
EntityTrapFaultID	Indicates the error code.

Impact on the System

All services on the board will be interrupted.

Possible Causes

The board was powered off.

Procedure

Replace the faulty board.

Related Information

None

3.2.3.2 ALM-303046710 A card has stopped working 132627

Description

SRM_ENTITY/1/BOARDINVALID: OID 1.3.6.1.4.1.2011.5.25.219.2.2.5 The board totally failed. (EntityPhysicalIndex=[integer], EntityPhysicalIndex=[integer], EntPhysicalName="[STRING]", EntityType=[integer], EntityTrapFaultID=132627)

SRM_ENTITY/1/BOARDINVALID: OID 1.3.6.1.4.1.2011.5.25.219.2.2.5 The board totally failed.(Index=[integer], EntityPhysicalIndex=[integer], PhysicalName="[STRING]", EntityTrapEntType=[integer], EntityTrapFaultID=132627)

The board experienced a complete failure.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046710	Critical	equipmentAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
EntityPhysicalIndex	Indicates the index of the physical entity.
EntityPhysicalIndexEntityPhysicalIndex	Indicates the index of the physical entity.

Name	Meaning
EntPhysicalNamePhysicalName	Indicates the name of the physical entity, such as "SFU LPU MPU slot <slotID>". The entity name varies according to the board type, such as the SFU, LPU, and MPU.
EntityTypeEntityTrapEntType	Indicates the type of the entity, such as mpu(1), lpu(2), sfu(3), pic(4), cfc card(5), and ofc(6).
EntityTrapFaultID	Indicates the error code.

Impact on the System

All services on the board will be interrupted and a speedy solution is required.

Possible Causes

Board registration failed.

Procedure

Collect information about alarms, logs, and configurations, and then contact Huawei technical support personnel.

Related Information

None

3.2.4 ALM-303046713 The power supply is invalid

Description

SRM_ENTITY/1/POWERINVALID: OID 1.3.6.1.4.1.2011.5.25.219.2.5.5 Power is invalid for some reason. (Index=[integer], EntityPhysicalIndex=[integer], EntPhysicalName="[STRING]", EntityTrapFaultID=136966)

The power supply module failed.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046713	Critical	equipmentAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
Index	Indicates the index.
EntityPhysicalIndex	Indicates the physical entity index.
EntPhysicalName	Indicates the physical entity name.
EntityType	Indicates the entity type.
EntityTrapFaultID	Indicates the error code.

Impact on the System

- For 1 U devices, services were not affected, but the system reliability was degraded.
- For 3 U devices, the power decreased, the chassis failed to run properly, and the reliability was degraded.

Possible Causes

Cause 1: The power module is switched off.

Cause 2: The power module fails.

Procedure

Step 1 Check whether the power module is switched off.

- Y => 2
- N => 3

Step 2 Switch on the power module.

Step 3 Check whether proper power supply is provided for the device.

- Y => 4
- N => 5

Step 4 Replace the power module if the power module is faulty.

Step 5 Run the **display device** command and check whether the power module status is **Normal**.

- Y => 6
- N => 4

Step 6 End.

----End

Related Information

None

3.2.5 ALM-303046700 The fan module is invalid

Description

SRM_ENTITY/2/FANINVALID: OID 1.3.6.1.4.1.2011.5.25.219.2.6.5 The fan module failed. (EntityPhysicalIndex=[integer], EntityPhysicalIndex=[integer], EntPhysicalName="[STRING]", EntityTrapFaultID=139264)

The fan module experienced a complete failure.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046700	Major	equipmentAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
EntityPhysicalIndex	Indicates the index of the physical entity.
EntPhysicalName	Indicates the name of the physical entity, such as "SFU LPU MPU slot <slotID>". The entity name varies according to the board type, such as the SFU, LPU, and MPU.
EntityTrapFaultID	Indicates the error code.

Impact on the System

This problem affects heat dissipation of the router; it will not affect services in a short time period but needs a speedy solution.

Possible Causes

The hardware of the fan module was faulty.

Procedure

Step 1 Check whether the fan module is properly installed in the slot.

Step 2 If so, replace the fan module; otherwise, install the fan module properly.

----End

Related Information

None

3.2.6 ALM-303046698 The card or subcard temperature is too high 143617

Description

SRM_ENTITY/6/ENTITYBRDTEMPALARM:OID 1.3.6.1.4.1.2011.5.25.219.2.10.13
Temperature rise over or fall below the warning alarm threshold. (Index=[integer], EntityPhysicalIndex=[integer], PhysicalName="[STRING]", EntityThresholdType=[integer], EntityThresholdValue=[integer], EntityThresholdCurrent=[integer], EntityTrapFaultID=143617)

The board or subcard temperature was too high.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046698	Major	equipmentAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
Index	Indicates the index.
EntityPhysicalIndex	Indicates the physical entity index.
EntPhysicalName	Indicates the physical entity name.
EntityType	Indicates the entity type.
EntityTrapFaultID	Indicates the error code.

Impact on the System

The device may be restarted, causing service interruption.

Possible Causes

Cause 1: The board temperature exceeds the upper alert threshold.

Cause 2: The fan is faulty.

Procedure

- Step 1** Run the **display device** command and check whether the fan status restores normal.
- Y =>2
 - N =>3
- Step 2** Lower the ambient temperature, run the **display temperature all** command, and check whether the board temperature is **Normal**.
- Y =>4
 - N =>3
- Step 3** Collect the information about alarms, logs, and configurations, and then contact Huawei technical support personnel.
- Step 4** End.
- End

Related Information

None

3.2.7 ALM-135462939 The fan module is removed

Description

SRM_ENTITY/1/FANREMOVE: OID 1.3.6.1.4.1.2011.5.25.219.2.6.1 Fan has been removed.(Index=[integer], EntityPhysicalIndex=[integer], EntPhysicalName="[STRING]", EntityTrapFaultID=137216)

The fan module was removed.

Attribute

Alarm ID	Alarm Severity	Alarm Type
135462939	Critical	equipmentAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
Index	Indicates the index.
EntityPhysicalIndex	Indicates the physical entity index.

Name	Meaning
EntPhysicalName	Indicates the physical entity name.
EntityType	Indicates the entity type.
EntityTrapFaultID	Indicates the error code.

Impact on the System

The device is overheated, and services will be interrupted.

Possible Causes

The fan module was removed.

Procedure

Step 1 Check whether the fan module needs to be replaced.

- Y => 2
- N => 3

Step 2 Insert a fan module immediately.

Step 3 Collect the information about alarms, logs, and configurations, and then contact Huawei technical support personnel.

Step 4 End.

----End

Related Information

None

3.3 V200 LSW Alarms

3.3.1 ALM-135462942 The optical module is invalid

3.3.1.1 ALM-135462942 The optical module is invalid 136193

Description

ENTITYTRAP/3/OPTPWRALM: OID [OID] The optical power exceeds the upper alarm threshold or falls below the lower alarm threshold. (Index=[INTEGER], EntityPhysicalIndex=[INTEGER], PhysicalName="[OCTET]", EntityTrapFaultID=[INTEGER], EntityTrapReasonDescr="[OCTET]")

The transmit power of an optical module is too high.

Attribute

Alarm ID	Alarm Severity	Alarm Type
135462942	Minor	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
Index	Indicates the index.
EntityPhysicalIndex	Indicates the index of the physical entity.
PhysicalName	Indicates the name of the physical entity.
EntityTrapFaultID	Indicates the error code.
EntityTrapReasonDescr	Indicates the description of the alarm cause.

Impact on the System

This alarm does not affect system operating if the interface on which the optical module is installed works properly.

Possible Causes

The transmit power of the optical module is too high.

Procedure

- Step 1** Run the **display transceiver slot *slot-id* verbose** command in the system view to check whether the transmit power **Tx Power** of the optical module is within the allowed range.
- If so, services are not affected. Collect alarms, logs, and configurations and contact technical support personnel.
 - If not, go to step 2.
- Step 2** Use an optical attenuator to reduce the transmit power of the optical module to the acceptable range. Check whether the alarm is cleared.
- If so, the alarm handling ends.
 - If not, go to step 3.
- Step 3** Replace the optical module, and check whether the alarm is cleared.

- If so, the alarm handling ends.
 - If not, collect alarms, logs, and configurations, and contact technical support personnel.
- End

Related Information

None

3.3.1.2 ALM-135462942 The optical module is invalid 136194

Description

ENTITYTRAP/3/OPTPWRALM: OID [OID] The optical power exceeds the upper alarm threshold or falls below the lower alarm threshold. (Index=[INTEGER], EntityPhysicalIndex=[INTEGER], PhysicalName="[OCTET]", EntityTrapFaultID=[INTEGER], EntityTrapReasonDescr="[OCTET]")

The transmit power of an optical module is too low.

Attribute

Alarm ID	Alarm Severity	Alarm Type
135462942	Minor	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
Index	Indicates the index.
EntityPhysicalIndex	Indicates the index of the physical entity.
PhysicalName	Indicates the name of the physical entity.
EntityTrapFaultID	Indicates the error code.
EntityTrapReasonDescr	Indicates the description of the alarm cause.

Impact on the System

This alarm does not affect system operating if the interface on which the optical module is installed works properly.

Possible Causes

The transmit power of the optical module is too low.

Procedure

Step 1 Run the **display transceiver slot slot-id verbose** command in the system view to check whether the transmit power **Tx Power** of the optical module is within the allowed range.

- If so, services are not affected. Collect alarms, logs, and configurations and contact technical support personnel.
- If not, go to step 2.

Step 2 Replace the optical module, and check whether the alarm is cleared.

- If so, the alarm handling ends.
- If not, collect alarms, logs, and configurations, and contact technical support personnel.

----End

Related Information

None

3.3.1.3 ALM-135462942 The optical module is invalid 136195

Description

ENTITYTRAP/3/OPTPWRALM: OID [OID] The optical power exceeds the upper alarm threshold or falls below the lower alarm threshold. (Index=[INTEGER], EntityPhysicalIndex=[INTEGER], PhysicalName="[OCTET]", EntityTrapFaultID=[INTEGER], EntityTrapReasonDescr="[OCTET]")

The receive power of an optical module is too high.

Attribute

Alarm ID	Alarm Severity	Alarm Type
135462942	Minor	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
Index	Indicates the index.

Name	Meaning
EntityPhysicalIndex	Indicates the index of the physical entity.
PhysicalName	Indicates the name of the physical entity.
EntityTrapFaultID	Indicates the error code.
136195	Indicates that the receive power of the optical module is too high.
EntityTrapReasonDescr	Indicates the description of the alarm cause.

Impact on the System

This alarm does not affect system operating if the interface on which the optical module is installed works properly.

Possible Causes

The receive power is too high.

Procedure

- Step 1** Run the **display transceiver slot *slot-id* verbose** command in the system view to check whether the receive power **Rx Power** of the optical module is within the allowed range.
- If so, collect alarms, logs, and configurations, and contact technical support personnel.
 - If not, go to step 2.
- Step 2** Check whether an alarm is generated for high transmit power on the peer optical module. If so, rectify the peer optical module fault first.
- Step 3** Check whether the peer optical module and the local optical module are of the same type. If not, replace the local optical module with a new one to ensure they are of the same type.
- Step 4** Add -5 dBm (recommended) attenuators to the optical module.
- Step 5** If the problem persists after the preceding steps, collect alarms, logs, and configurations, and contact technical support personnel.

----End

Related Information

None

3.3.1.4 ALM-135462942 The optical module is invalid 136196

Description

ENTITYTRAP/3/OPTPWALM: OID [OID] The optical power exceeds the upper alarm threshold or falls below the lower alarm threshold. (Index=[INTEGER], EntityPhysicalIndex=[INTEGER], PhysicalName="[OCTET]", EntityTrapFaultID=[INTEGER], EntityTrapReasonDescr="[OCTET]")

The receive power of an optical module is too low.

Attribute

Alarm ID	Alarm Severity	Alarm Type
135462942	Minor	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
Index	Indicates the index.
EntityPhysicalIndex	Indicates the index of the physical entity.
PhysicalName	Indicates the name of the physical entity.
EntityTrapFaultID	Indicates the error code.
EntityTrapReasonDescr	Indicates the description of the alarm cause.

Impact on the System

This alarm does not affect system operating if the interface on which the optical module is installed works properly.

Possible Causes

The receive power of the optical module was too low.

Procedure

- Step 1
- Run the **display transceiver slot *slot-id* verbose** command in the system view to check whether the receive power **Rx Power** of the local interface is within the acceptable range.

- If so, collect alarms, logs, and configurations, and contact technical support personnel.
 - If not, go to step 2.
- Step 2** Check whether the peer port is physically Up and whether there is no alarm indicating that the transmit power is too low.
- If so, perform an external loopback test on the interface. If the interface is in Up state, perform loopback tests on the nodes along the transmission path to locate the failure point or link. Then check whether the alarm is cleared. If not, go to 3.
 - If not, go to step 3.
- Step 3** Check whether the peer port is physically Down and a corresponding alarm is generated, rectify the fault on the peer port.
- If so, repair the peer port. Check whether the alarm is cleared. If not, go to step 5.
 - If not, go to step 4.
- Step 4** Test whether the fiber is working normally.
- If so, replace the fiber and check whether the alarm is cleared. If not, go to step 6.
 - If not, go to step 5.
- Step 5** Replace the optical module of the local port and check whether the alarm is cleared.
- If so, the alarm handling ends.
 - If not, go to step 6.
- Step 6** Collect alarms, logs, and configurations, and contact technical support personnel.
- End

Related Information

None

3.3.1.5 ALM-135462942 The optical module is invalid 136201

Description

ENTITYTRAP/3/OPTTEMALM:OID [OID] The temperature of optical exceeds the upper alarm threshold or falls below the lower alarm threshold.
(Index=[INTEGER], EntityPhysicalIndex=[INTEGER], PhysicalName="[OCTET]", EntityTrapFaultID=[INTEGER], EntityTrapReasonDescr="[OCTET]")

The optical module temperature exceeds the upper threshold.

Attribute

Alarm ID	Alarm Severity	Alarm Type
135462942	Minor	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
Index	Indicates the index.
EntityPhysicalIndex	Indicates the index of the physical entity.
PhysicalName	Indicates the name of the physical entity.
EntityTrapFaultID	Indicates the error code.
EntityTrapReasonDescr	Indicates the description of the alarm cause.

Impact on the System

The optical module may fail to work properly, affecting services.

Possible Causes

The possible causes include:

- The device is not ventilated well, which causes heat unable to be dissipated.
- The air filter is blocked by dust.
- Vacant slots are not covered with filler panels.
- The ambient temperature of the device is too high.
- The number of fans on the device is insufficient.
- Fans on the device are faulty.

Procedure

- Step 1** Clean the air vent and check whether the alarm is cleared.
- If so, the alarm handling ends.
 - If not, go to step 2.
- Step 2** Reduce the ambient temperature and check whether the alarm is cleared.
- If so, the alarm handling ends.
 - If not, go to step 3.
- Step 3** Run the **display fan** command to check the fan status. Ensure that fans are working normally and check whether the alarm is cleared.
- If so, the alarm handling ends.

- If not, go to step 4.

Step 4 Add fans and check whether the alarm is rectified.

- If so, the alarm handling ends.
- If not, collect alarm and configuration information, and contact technical support personnel.

----End

Related Information

None

3.3.1.6 ALM-135462942 The optical module is invalid 136202

Description

ENTITYTRAP/3/OPTTEMALM:OID [OID] The temperature of optical exceeds the upper alarm threshold or falls below the lower alarm threshold.
(Index=[INTEGER], EntityPhysicalIndex=[INTEGER], PhysicalName="[OCTET]", EntityTrapFaultID=[INTEGER], EntityTrapReasonDescr="[OCTET]")

The optical module temperature is below the lower threshold.

Attribute

Alarm ID	Alarm Severity	Alarm Type
135462942	Minor	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
Index	Indicates the index.
EntityPhysicalIndex	Indicates the index of the physical entity.
PhysicalName	Indicates the name of the physical entity.
EntityTrapFaultID	Indicates the error code.
EntityTrapReasonDescr	Indicates the description of the alarm cause.

Impact on the System

The optical module may fail to work properly, affecting services.

Possible Causes

The ambient temperature is too low.

Procedure

Run the **display transceiver slot *slot-id* verbose** command to check whether the temperature of the optical module is within the allowed range.

- If the temperature of the optical module is within the allowed range, collect alarms, logs, and configurations, and contact technical support personnel.
- If the temperature of the optical module is out of the allowed range, replace the optical module.

Related Information

None

3.3.1.7 ALM-135462942 The optical module is invalid 136203

Description

ENTITYTRAP/3/OPTICALINVALID: OID [OID] Optical Module is invalid.
(Index=[INTEGER], EntityPhysicalIndex=[INTEGER], PhysicalName="[OCTET]", EntityTrapFaultID=[INTEGER], EntityTrapReasonDescr="[OCTET]")

The optical module fails.

Attribute

Alarm ID	Alarm Severity	Alarm Type
135462942	Minor	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
Index	Indicates the index.
EntityPhysicalIndex	Indicates the index of the physical entity.
PhysicalName	Indicates the name of the physical entity.

Name	Meaning
EntityTrapFaultID	Indicates the error code.
EntityTrapReasonDescr	Indicates the description of the alarm cause.

Impact on the System

Services on the interface may be interrupted.

Possible Causes

An unsupported optical module is installed in the optical interface. For example, an XGE optical module is installed in a GE optical interface; a 100GE optical module is installed in a 40GE optical interface.

Procedure

Remove the optical module or replace it with an optical interface-supported optical module.

Related Information

None

3.3.1.8 ALM-135462942 The optical module is invalid 136220

Description

ENTITYTRAP/3/OPTMAYINVALID: OID [OID] The optical power exceeds the upper warning threshold or falls below the lower warning threshold. (Index=[INTEGER], EntityPhysicalIndex=[INTEGER], PhysicalName="[OCTET]", EntityTrapFaultID=[INTEGER], EntityTrapReasonDescr="[OCTET]")

The transmit power of an optical module is too high.

Attribute

Alarm ID	Alarm Severity	Alarm Type
135462942	Minor	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.

Name	Meaning
Index	Indicates the index.
EntityPhysicalIndex	Indicates the index of the physical entity.
PhysicalName	Indicates the name of the physical entity.
EntityTrapFaultID	Indicates the error code.
EntityTrapReasonDescr	Indicates the description of the alarm cause.

Impact on the System

This alarm does not affect system operating if the interface on which the optical module is installed works properly.

Possible Causes

The transmit power of the optical module is too high.

Procedure

- Step 1** Run the **display transceiver slot *slot-id* verbose** command in the system view to check whether the transmit power **Tx Power** of the optical module is within the allowed range.
- If so, services are not affected. Collect alarms, logs, and configurations and contact technical support personnel.
 - If not, go to step 2.
- Step 2** Use an optical attenuator to reduce the transmit power of the optical module to the acceptable range. Check whether the alarm is cleared.
- If so, the alarm handling ends.
 - If not, go to step 3.
- Step 3** Replace the optical module, and check whether the alarm is cleared.
- If so, the alarm handling ends.
 - If not, collect alarms, logs, and configurations, and contact technical support personnel.

----End

Related Information

None

3.3.1.9 ALM-135462942 The optical module is invalid 136221

Description

ENTITYTRAP/3/OPTMAYINVALID: OID [OID] The optical power exceeds the upper warning threshold or falls below the lower warning threshold. (Index=[INTEGER], EntityPhysicalIndex=[INTEGER], PhysicalName="[OCTET]", EntityTrapFaultID=[INTEGER], EntityTrapReasonDescr="[OCTET]")

The transmit power of an optical module is too low.

Attribute

Alarm ID	Alarm Severity	Alarm Type
135462942	Minor	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
Index	Indicates the index.
EntityPhysicalIndex	Indicates the index of the physical entity.
PhysicalName	Indicates the name of the physical entity.
EntityTrapFaultID	Indicates the error code.
EntityTrapReasonDescr	Indicates the description of the alarm cause.

Impact on the System

This alarm does not affect system operating if the interface on which the optical module is installed works properly.

Possible Causes

The transmit power of the optical module is too low.

Procedure

- Step 1** Run the **display transceiver slot slot-id verbose** command in the system view to check whether the transmit power **Tx Power** of the optical module is within the allowed range.

- If so, services are not affected. Collect alarms, logs, and configurations and contact technical support personnel.
- If not, go to step 2.

Step 2 Replace the optical module, and check whether the alarm is cleared.

- If so, the alarm handling ends.
- If not, collect alarms, logs, and configurations, and contact technical support personnel.

----End

Related Information

None

3.3.1.10 ALM-135462942 The optical module is invalid 136222

Description

ENTITYTRAP/3/OPTMAYINVALID: OID [OID] The optical power exceeds the upper warning threshold or falls below the lower warning threshold. (Index=[INTEGER], EntityPhysicalIndex=[INTEGER], PhysicalName="[OCTET]", EntityTrapFaultID=[INTEGER], EntityTrapReasonDescr="[OCTET]")

The receive power of an optical module is too high.

Attribute

Alarm ID	Alarm Severity	Alarm Type
135462942	Minor	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
Index	Indicates the index.
EntityPhysicalIndex	Indicates the index of the physical entity.
PhysicalName	Indicates the name of the physical entity.
EntityTrapFaultID	Indicates the error code.
EntityTrapReasonDescr	Indicates the description of the alarm cause.

Impact on the System

This alarm does not affect system operating if the interface on which the optical module is installed works properly.

Possible Causes

The receive power is too high.

Procedure

- Step 1** Run the **display transceiver slot *slot-id* verbose** command in the system view to check whether the receive power **Rx Power** of the optical module is within the allowed range.
- If so, collect alarms, logs, and configurations, and contact technical support personnel.
 - If not, go to step 2.
- Step 2** Check whether an alarm is generated for high transmit power on the peer optical module. If so, rectify the peer optical module fault first.
- Step 3** Check whether the peer optical module and the local optical module are of the same type. If not, replace the local optical module with a new one to ensure they are of the same type.
- Step 4** Add -5 dBm (recommended) attenuators to the optical module.
- Step 5** If the problem persists after the preceding steps, collect alarms, logs, and configurations, and contact technical support personnel.

----End

Related Information

None

3.3.1.11 ALM-135462942 The optical module is invalid 136223

Description

ENTITYTRAP/3/OPTMAYINVALID: OID [OID] The optical power exceeds the upper warning threshold or falls below the lower warning threshold. (Index=[INTEGER], EntityPhysicalIndex=[INTEGER], PhysicalName="[OCTET]", EntityTrapFaultID=[INTEGER], EntityTrapReasonDescr="[OCTET]")

The receive power of an optical module is too low.

Attribute

Alarm ID	Alarm Severity	Alarm Type
135462942	Minor	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
Index	Indicates the index.
EntityPhysicalIndex	Indicates the index of the physical entity.
PhysicalName	Indicates the name of the physical entity.
EntityTrapFaultID	Indicates the error code.
EntityTrapReasonDescr	Indicates the description of the alarm cause.

Impact on the System

This alarm does not affect system operating if the interface on which the optical module is installed works properly.

Possible Causes

The receive power of the optical module was too low.

Procedure

- Step 1** Run the **display transceiver slot *slot-id* verbose** command in the system view to check whether the receive power **Rx Power** of the local interface is within the acceptable range.
- If so, collect alarms, logs, and configurations, and contact technical support personnel.
 - If not, go to step 2.
- Step 2** Check whether the peer port is physically Up and whether there is no alarm indicating that the transmit power is too low.
- If so, perform an external loopback test on the interface. If the interface is in Up state, perform loopback tests on the nodes along the transmission path to locate the failure point or link. Then check whether the alarm is cleared. If not, go to 3.
 - If not, go to step 3.
- Step 3** Check whether the peer port is physically Down and a corresponding alarm is generated, rectify the fault on the peer port.
- If so, repair the pee port. Check whether the alarm is cleared. If not, go to step 5.
 - If not, go to step 4.

- Step 4**
Test whether the fiber is working normally.
 - If so, replace the fiber and check whether the alarm is cleared. If not, go to step 6.
 - If not, go to step 5.
- Step 5**
Replace the optical module of the local port and check whether the alarm is cleared.
 - If so, the alarm handling ends.
 - If not, go to step 6.
- Step 6**
Collect alarms, logs, and configurations, and contact technical support personnel.
- End

Related Information

None

3.3.1.12 ALM-135462942 The optical module is invalid 136224

Description

ENTITYTRAP/3/OPTMAYINVALID: OID [OID] The optical module may be invalid. (Index=[INTEGER], EntityPhysicalIndex=[INTEGER], PhysicalName=\"[OCTET]\", EntityTrapFaultID=[INTEGER], EntityTrapReasonDescr=\"[OCTET]\")

The optical module failed CRC check.

Attribute

Alarm ID	Alarm Severity	Alarm Type
135462942	Minor	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
Index	Indicates the index.
EntityPhysicalIndex	Indicates the index of the physical entity.
PhysicalName	Indicates the name of the physical entity.
EntityTrapFaultID	Indicates the error code.

Name	Meaning
EntityTrapReasonDescr	Indicates the description of the alarm cause.

Impact on the System

The optical interface may fail to go Up.

Possible Causes

Optical module information is incorrect.

Procedure

Run the **display transceiver** *interface-type interface-number* command to obtain optical module information and contact technical support personnel.

Related Information

None

3.3.2 ALM-303046703 The power supply is removed 136448

Description

ENTITYTRAP/4/POWERREMOVE: OID [OID] Power is absent. (Index=[INTEGER], EntityPhysicalIndex=[INTEGER], PhysicalName="[OCTET]", EntityTrapFaultID=[INTEGER])

The power supply was removed.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046703	Warning	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
Index	Indicates the index.
EntityPhysicalIndex	Indicates the index of the physical entity.

Name	Meaning
PhysicalName	Indicates the name of the physical entity.
EntityTrapFaultID	Indicates the error code.

Impact on the System

Some boards cannot work properly due to lack of power.

Possible Causes

The power supply was removed.

Procedure

- Step 1
- Check whether the power module is installed in the slot.
 - If so, go to step 2.
 - If not, install the power module in the slot.
- Step 2
- Run the **display device** command to check whether the power module is working properly.
 - If so, but the alarm persists, replace the power module.
 - If not, install the power module securely.
- End

Related Information

[3.3.3 ALM-303046702 The power module is installed 136448](#)

3.3.3 ALM-303046702 The power module is installed 136448

Description

ENTITYTRAP/4/POWERINSERT: OID [OID] Power is present. (Index=[INTEGER], EntityPhysicalIndex=[INTEGER], PhysicalName="[OCTET]", EntityTrapFaultID=[INTEGER])

The power supply was inserted.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046702	Warning	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
Index	Indicates the index.
EntityPhysicalIndex	Indicates the index of the physical entity.
PhysicalName	Indicates the name of the physical entity.
EntityTrapFaultID	Indicates the error code.

Impact on the System

None

Possible Causes

The power supply was inserted.

Procedure

This alarm is informational and no action is required.

Related Information

[3.3.2 ALM-303046703 The power supply is removed 136448](#)

3.3.4 ALM-303046701 Power supply is invalid

3.3.4.1 ALM-303046701 Power supply is invalid 136961

Description

Entitytrap/1/POWERINVALID: OID [OID] Power supply is unavailable for some reason.(Index=[INTEGER], EntityPhysicalIndex=[INTEGER], PhysicalName= \"[OCTET]\", EntityTrapFaultID=[INTEGER])

The power supply is invalid.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046701	Critical	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
Index	Indicates the index.
EntityPhysicalIndex	Indicates the index of the physical entity.
PhysicalName	Indicates the entity name.
EntityTrapFaultID	Indicates the error code.

Impact on the System

The device may be powered off because of power insufficiency.

Possible Causes

The power module does not work properly.

Procedure

Replace the power module.

Related Information

None

3.3.4.2 ALM-303046701 Power supply is invalid 136966

Description

ENTITYTRAP/1/POWERINVALID: OID [OID] Power supply is unavailable for some reason. (Index=[INTEGER], EntityPhysicalIndex=[INTEGER], PhysicalName="[OCTET]", EntityTrapFaultID=[INTEGER])

The power supply is invalid.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046701	Critical	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
Index	Indicates the index.
EntityPhysicalIndex	Indicates the index of the physical entity.
PhysicalName	Indicates the entity name.
EntityTrapFaultID	Indicates the error code.

Impact on the System

Boards may fail to be powered on due to insufficient power supply

Possible Causes

Cause 1: The power supply was installed but not powered on.

Cause 2: The power module in the switch has failed.

Procedure

- Rectify the fault according to [A Power Module Cannot Provide Power](#) in the *Revelations of Troubleshooting-Campus Switch-Hardware Fault*.

Related Information

None

3.3.4.3 ALM-303046701 Power supply is invalid 136969

Description

ENTITYTRAP/1/POWERINVALID: OID [OID] Power supply is unavailable for some reason.(Index=[INTEGER], EntityPhysicalIndex=[INTEGER], PhysicalName="[OCTET]", EntityTrapFaultID=[INTEGER])

A power module experienced a complete failure.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046701	Critical	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
Index	Indicates the index of the alarm.
EntityPhysicalIndex	Indicates the index of a physical entity.
PhysicalName	Indicates the physical entity name.
EntityTrapFaultID	Indicates the error code.

Impact on the System

The device may be powered off because of power insufficiency.

Possible Causes

Cause 1: The power switch on the power module is turned off.

Cause 2: No power cable is connected to the power module.

Cause 3: The output voltage of the external power supply system is out of the input voltage range required for the chassis.

Procedure

Step 1 Check that the power module is connected to the external power supply system correctly and turn on the power switch of the power module. Check whether the alarm is cleared.

If so, the alarm handling ends.

If not, go to step 2.

Step 2 Check whether the output voltage of the external power supply system is within the input voltage range required for the chassis. For the input voltage ranges required for each chassis, see Hardware Description > Chassis > Specifications.

If not, ask power line maintenance personnel to check the power supply lines.

If so, go to step 3.

Step 3 Contact technical support personnel.

----End

Related Information

None

3.3.4.4 ALM-303046701 Power supply is invalid 136972

Description

ENTITYTRAP/1/POWERINVALID: OID [OID] Power supply is unavailable for some reason.(Index=[INTEGER], EntityPhysicalIndex=[INTEGER], PhysicalName="[OCTET]", EntityTrapFaultID=[INTEGER])

The power supply is invalid.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046701	Critical	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
Index	Indicates the index.
EntityPhysicalIndex	Indicates the index of the physical entity.
PhysicalName	Indicates the entity name.
EntityTrapFaultID	Indicates the error code.

Impact on the System

The PoE function does not take effect, and powered devices (PDs) cannot be powered on.

Possible Causes

The PoE power module is not supported by the device.

Procedure

Replace the power module with a PoE power module supported by the device. Currently, PoE power modules supported by a switch include 800 W AC, 2200 W AC, and 2200 W DC power modules.

Related Information

None

3.3.4.5 ALM-303046701 Power supply is invalid 136973

Description

ENTITYTRAP/1/POWERINVALID: OID [OID] Power supply is unavailable for some reason. (Index=[INTEGER], EntityPhysicalIndex=[INTEGER], PhysicalName="[OCTET]", EntityTrapFaultID=[INTEGER])

The power supply is invalid.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046701	Critical	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
Index	Indicates the index.
EntityPhysicalIndex	Indicates the index of the physical entity.
PhysicalName	Indicates the entity name.
EntityTrapFaultID	Indicates the error code.

Impact on the System

The switch may restart, affecting services.

Possible Causes

A power module providing mismatching power is installed in the switch. A 150 W power module is installed in an S5720HI.

Procedure

Replace the current power module with a power module providing matching power.

Related Information

None

3.3.4.6 ALM-303046701 Power supply is invalid 136984

Description

ENTITYTRAP/1/POWERINVALID: OID [OID] Power supply is unavailable for some reason.(Index=[INTEGER], EntityPhysicalIndex=[INTEGER], PhysicalName="[OCTET]", EntityTrapFaultID=[INTEGER])

The power supply experiences a complete failure.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046701	Critical	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
Index	Indicates an index.
EntityPhysicalIndex	Indicates the index of a physical entity.
PhysicalName	Indicates the name of the physical entity.
EntityTrapFaultID	Indicates the error code of the alarm, which is 136984.

Impact on the System

The RPS power supply is present but has no output power and so is unavailable.

Possible Causes

The RPS 12 V power supply is abnormal.

Procedure

Replace the RPS power supply.

Related Information

None

3.3.5 ALM-303046657 The fan module is removed 137216

Description

ENTITYTRAP/4/FANREMOVE: OID [OID] Fan has been removed.
(Index=[INTEGER], EntityPhysicalIndex=[INTEGER], PhysicalName="[OCTET]", EntityTrapFaultID=[INTEGER])

The fan is not installed properly.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046657	Warning	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
Index	Indicates the index.
EntityPhysicalIndex	Indicates the index of the physical entity.
PhysicalName	Indicates the name of the physical entity.
EntityTrapFaultID	Indicates the error code.

Impact on the System

The temperature of the device will increase due to deterioration of heat dissipation performance. Services are not affected in a short time, but the fault should be rectified quickly.

Possible Causes

The fan was removed or not installed properly.

Procedure

Step 1 Check whether the fan was manually removed for routine maintenance.

- If so, the alarm handling ends.
- If not, go to step 2.

Step 2 Run the **display device** command to check whether the fan is registered successfully.

- If so, collect alarm information and configuration information, and then contact technical support personnel.
- If not, go to step 3.

Step 3 Check whether the fan is installed securely.

- If so, collect alarm information and configuration information, and then contact technical support personnel.
- If not, install the fan securely and go to step 4.

Step 4 Check whether there is an alarm indicating that a fan is installed.

- If so, the alarm handling ends.
- If not, collect alarm information and configuration information, and then contact technical support personnel.

----End

Related Information

None

3.3.6 ALM-303046656 The fan is faulty

3.3.6.1 ALM-303046656 The fan is faulty 139264

Description

ENTITYTRAP/1/FANINVALID: OID [OID] Fan is invalid. (Index=[INTEGER], EntityPhysicalIndex=[INTEGER], PhysicalName="[OCTET]", EntityTrapFaultID=[INTEGER])

The fan is invalid.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046656	Critical	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
Index	Indicates the index.
EntityPhysicalIndex	Indicates the index of the physical entity.

Name	Meaning
PhysicalName	Indicates the name of the physical entity.
EntityTrapFaultID	Indicates the error code.

Impact on the System

The fan cannot work normally, so the temperature of boards will increase. As a result, the boards may be unable to work normally. For example, packet loss may occur or even the switch works abnormally or restarts.

Possible Causes

The fan hardware is faulty.

Procedure

Rectify the fault according to [A Fan Fails](#) in the *Revelations of Troubleshooting-Campus Switch-Hardware Fault*.

Related Information

None

3.3.6.2 ALM-303046656 The fan is faulty 139266

Description

ENTITYTRAP/1/FANINVALID: OID [OID] Fan is invalid. (Index=[INTEGER], EntityPhysicalIndex=[INTEGER], PhysicalName="[OCTET]", EntityTrapFaultID=[INTEGER])

The fan is invalid.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046656	Critical	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.

Name	Meaning
Index	Indicates the index.
EntityPhysicalIndex	Indicates the physical entity index.
PhysicalName	Indicates the physical entity name.
EntityTrapFaultID	Indicates the alarm error code.

Impact on the System

Temperature of a device may increase because performance of fans cannot meet the heat dissipation requirement of the chassis. As a result, the device may be unable to work normally. For example, packet loss may occur or even the switch works abnormally or restarts.

Possible Causes

The fan model inserted in an S6720EI, S6720S-EI does not match the chassis mode.

Procedure

- Replace the fan module with one matching the device model. S6720EI, S6720S-EI supports only two fan models FAN-060B-B and FAN-060C-B.

Related Information

None

3.3.7 ALM-303046661 The CPU usage of the device exceeds the alarm threshold

Description

ENTITYTRAP/4/ENTITYCPUALARM: OID [OID] CPU utilization exceeded the pre-alarm threshold. (Index=[INTEGER], EntityPhysicalIndex=[INTEGER], PhysicalName="[OCTET]", EntityThresholdType=[INTEGER], EntityThresholdValue=[INTEGER], EntityThresholdCurrent=[INTEGER], EntityTrapFaultID=[INTEGER].)

The CPU usage exceeds the alarm threshold.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046661	Warning	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
Index	Indicates the alarm ID.
EntityPhysicalIndex	Indicates the index of the physical entity where the alarm is reported.
PhysicalName	Indicates the physical entity name.
EntityThresholdType	Indicates the alarm type.
EntityThresholdValue	Indicates the alarm threshold.
EntityThresholdCurrent	Indicates the current CPU usage.
EntityTrapFaultID	Indicates the error code of the alarm.

Impact on the System

The high CPU usage will delay processing of some services.

Possible Causes

The CPU usage of the device exceeds the alarm threshold.

Procedure

Rectify the fault according to [CPU Usage Is High](#) in the *Revelations of Troubleshooting-Campus Switch-Device Management And Maintenance*.

Related Information

None

3.3.8 ALM-303046660 The memory usage of the device exceeds the alarm threshold

Description

ENTITYTRAP/4/ENTITYMEMORYALARM: OID [OID] Memory usage exceeded the threshold, and it may cause the system to reboot. (Index=[INTEGER], EntityPhysicalIndex=[INTEGER], PhysicalName="[OCTET]", EntityThresholdType=[INTEGER], EntityThresholdValue=[INTEGER], EntityThresholdCurrent=[INTEGER], EntityTrapFaultID= [INTEGER].)

The memory usage exceeds the alarm threshold.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046660	Warning	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
Index	Indicates the alarm ID.
EntityPhysicalIndex	Indicates the index of the physical entity where the alarm is reported.
PhysicalName	Indicates the physical entity name.
EntityThresholdType	Indicates the alarm type.
EntityThresholdValue	Indicates the alarm threshold.
EntityThresholdCurrent	Indicates the current memory usage.
EntityTrapFaultID	Indicates the error code of the alarm.

Impact on the System

The high memory usage will delay processing of some services.

Possible Causes

The memory usage of the device exceeds the alarm threshold.

Procedure

Rectify the fault according to [High Memory Usage](#) in the *Revelations of Troubleshooting-Campus Switch-Device Management And Maintenance*.

Related Information

None

3.3.9 ALM-303046659 The temperature is abnormal

3.3.9.1 ALM-303046659 The temperature is abnormal 140544

Description

ENTITYTRAP/1/ENTITYBRDTEMPALARM: OID [OID] Temperature rise over or fall below the warning alarm threshold. (Index=[INTEGER], EntityPhysicalIndex=[INTEGER], PhysicalName="[OCTET]", EntityThresholdType=[INTEGER], EntityThresholdValue=[INTEGER], EntityThresholdCurrent=[INTEGER], EntityTrapFaultID=[INTEGER])

The temperature of the board is higher than the upper threshold.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046659	Critical	environmentalAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
Index	Indicates the index.
EntityPhysicalIndex	Indicates the index of the physical entity.
PhysicalName	Indicates the name of the physical entity.
EntityThresholdType	Indicates the threshold type of the physical entity.
EntityThresholdValue	Indicates the threshold value of the physical entity.
EntityThresholdCurrent	Indicates the current value of the physical entity.
EntityTrapFaultID	Indicates the error code.

Impact on the System

Services on the switch may be affected if the temperature becomes too high.

Possible Causes

- The chassis is not ventilated well, which causes heat unable to be dissipated.

- The ambient temperature is high.
- There are not enough fans in the switch.
- One or more fans in the switch have failed.
- The upper threshold of the temperature is too low.

Procedure

- Step 1** Clean the air filter and remove the objects that block the air exhaust vents (if any). Cover all vacant slots with filler panels to ensure efficient heat dissipation. Then check whether the alarm is cleared.
- If so, the alarm handling ends.
 - If not, go to step 2.
- Step 2** Check whether the ambient temperature of the device is too high.
- If so, go to step 3.
 - If not, go to step 4.
- Step 3** Lower the temperature in the equipment room, and then go to step 4.
- Step 4** Check whether fans are properly installed in all fan slots.
- If so, go to step 6.
 - If not, go to step 5.
- Step 5** Increase the number of fans, and then go to step 6.
- Step 6** Run the **display fan** command to check the status of fans and determine whether any fan is faulty.
- If so, go to step 7.
 - If not, go to step 8.
- Step 7** Replace the faulty fan, and then go to step 8.
- Step 8** After the switch has been running for a period of time, run the **display temperature all** command to check whether temperature of the device is still high.
- If so, collect alarm information and configuration information, and then contact technical support personnel.
 - If not, the alarm handling ends.
- End

Related Information

None

3.3.9.2 ALM-303046659 The temperature is abnormal 140545

Description

ENTITYTRAP/1/ENTITYBRDTEMPALARM: OID [OID] Temperature rise over or fall below the warning alarm threshold. (Index=[INTEGER],

EntityPhysicalIndex=[INTEGER], PhysicalName="[OCTET]",
EntityThresholdType=[INTEGER], EntityThresholdValue=[INTEGER],
EntityThresholdCurrent=[INTEGER], EntityTrapFaultID=[INTEGER])

The temperature of the board falls below the lower threshold.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046659	Critical	environmentalAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
Index	Indicates the index.
EntityPhysicalIndex	Indicates the index of the physical entity.
PhysicalName	Indicates the name of the physical entity.
EntityThresholdType	Indicates the threshold type of the physical entity.
EntityThresholdValue	Indicates the threshold value of the physical entity.
EntityThresholdCurrent	Indicates the current value of the physical entity.
EntityTrapFaultID	Indicates the error code.

Impact on the System

Services on the board may be affected if the temperature becomes too low.

Possible Causes

The ambient temperature is too low.

Procedure

- Step 1** Measure the ambient temperature. If the ambient temperature is too low, use air conditioners or heaters to increase the temperature.

Step 2 If the ambient temperature is normal, the lower threshold of the temperature may be too high. Run the **temperature threshold slot slotid lower-limit lower upper-limit upper** command to decrease the lower threshold of the temperature.

----End

Related Information

None

3.3.9.3 ALM-303046659 The temperature is abnormal 143624

Description

ENTITYTRAP/1/ENTITYBRDTEMPALARM: OID [OID] Temperature rise over or fall below the warning alarm threshold. (Index=[INTEGER], EntityPhysicalIndex=[INTEGER], PhysicalName="[OCTET]", EntityThresholdType=[INTEGER], EntityThresholdValue=[INTEGER], EntityThresholdCurrent=[INTEGER], EntityTrapFaultID=[INTEGER])

The temperature of the chip is higher than the upper threshold.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046659	Critical	environmentalAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
Index	Indicates the index.
EntityPhysicalIndex	Indicates the index of the physical entity.
PhysicalName	Indicates the name of the physical entity.
EntityThresholdType	Indicates the threshold type of the physical entity.
EntityThresholdValue	Indicates the threshold value of the physical entity.
EntityThresholdCurrent	Indicates the current value of the physical entity.
EntityTrapFaultID	Indicates the error code.

Impact on the System

Services on the switch may be affected if the chip temperature becomes too high.

Possible Causes

- The chassis is not ventilated well, which causes heat unable to be dissipated.
- Rear card slots are not covered with filler panels.
- The ambient temperature is high.
- There are not enough fans in the switch.
- One or more fans in the switch have failed.

Procedure

Step 1 Clean the air vent and check whether the alarm is cleared.

- (1) If so, go to step 7.
- (2) If not, go to step 2.

Step 2 Install filler panels in rear card slots and check whether the alarm is cleared.

- (1) If so, go to step 7.
- (2) If not, go to step 3.

Step 3 Reduce the ambient temperature and check whether the alarm is cleared.

- (1) If so, go to step 7.
- (2) If not, go to step 4.

Step 4 Run the **display fan** command to check the fan status. Ensure that fans are working normally and check whether the alarm is cleared.

- (1) If so, go to step 7.
- (2) If not, go to step 5.

Step 5 Add fans and check whether the alarm is rectified.

- (1) If so, go to step 7.
- (2) If not, go to step 6.

Step 6 Contact technical support personnel.

Step 7 End.

----End

Related Information

None

3.3.10 ALM-303046658 The PD connected to the interface is powered off

Description

POE/4/POWEROFF: OID [OID] PD powered off.(IfIndex=[INTEGER], Interface="[OCTET"])

The PD connected to the interface is powered off.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046658	Warning	Communication alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
IfIndex	Indicates the interface index.
Interface	Indicates the interface name.

Impact on the System

The PD connected to the interface is powered off and cannot work normally.

Possible Causes

1. The PD is removed.
2. The PD is faulty.
3. When the power is insufficient, the interface with a higher priority preempts the power.
4. The interface to which the PD connects is automatically powered off in the power-off time range.
5. The PD is powered off because of overcurrent protection.

Procedure

Step 1 Check whether the PD is removed.

If so, go to step 2.

If not, go to step 4.

- Step 2** Check whether the PD is removed because of a normal operation.
- If so, the alarm handling ends.
- If not, go to step 3.
- Step 3** Install the PD to check whether it is powered on.
- If so, the alarm handling ends.
- If not, go to step 4.
- Step 4** Run the **display poe power-state** *interface-type interface-number* command to check whether the maximum output power of the interface is sufficient.
- If so, go to step 5.
- If not, connect the PD to another interface or PoE device.
- Step 5** Run the **display poe power-state** *interface-type interface-number* command to check whether the power supply priority of the interface is low.
- If so, go to step 6.
- If not, go to step 8.
- Step 6** Check whether the power supply priority of the interface needs to be reconfigured.
- If so, go to step 6.
- If not, go to step 7.
- Step 7** Run the **poe priority** command to configure the power supply priority of the interface. Then check whether the PD is powered on.
- If so, the alarm handling ends.
- If not, go to step 8.
- Step 8** Run the **display poe power-state** *interface-type interface-number* command to check whether the interface is in the power-off time range.
- If so, the alarm handling ends.
- If not, go to step 9.
- Step 9** Check whether the PD is faulty.
- If so, replace it.
- If not, collect alarm information and configuration information, and then contact technical support personnel.
- End

Related Information

[3.3.11 ALM-303046665 PoE power supply is enabled on the port](#)

3.3.11 ALM-303046665 PoE power supply is enabled on the port

Description

POE/4/POWERON: OID [OID] PD powered on.(IfIndex=[INTEGER], Interface="[OCTET"])

The interface meets the following power supply conditions:

1. The power is sufficient.
2. The PD is identified by the system.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046665	Warning	Communication alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
IfIndex	Indicates the interface index.
Interface	Indicates the interface name.

Impact on the System

Services are not affected.

Possible Causes

The alarm recovery message is generated after power-off.

Procedure

This alarm indicates that a fault is rectified, and no action is required.

Related Information

[3.3.10 ALM-303046658 The PD connected to the interface is powered off](#)

3.3.12 ALM-134807555 The PD is connected

Description

POE/4/PDCONNECT: OID [OID] PD connected.(IfIndex=[INTEGER], Interface="[OCTET"])

The PD is connected to an interface.

Attribute

Alarm ID	Alarm Severity	Alarm Type
134807555	Warning	Communication alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
IfIndex	Indicates the interface index.
Interface	Indicates the interface name.

Impact on the System

Services are not affected.

Possible Causes

The system detects a valid PD.

Procedure

A new PD is added. This alarm is informational and no action is required.

Related Information

[3.3.13 ALM-303046664 This PD is disconnected](#)

3.3.13 ALM-303046664 This PD is disconnected

Description

POE/4/PDDISCONNECT: OID [OID] PD disconnected.(IfIndex=[INTEGER], Interface="[OCTET"])

The PD is disconnected from an interface.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046664	Warning	Communication alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
IfIndex	Indicates the interface index.
Interface	Indicates the interface name.

Impact on the System

The PD is unavailable and services are not affected.

Possible Causes

A valid PD is removed.

Procedure

Check whether the PD needs to be removed.

If so, the alarm handling ends.

If not, reinstall the PD.

Related Information

[3.3.12 ALM-134807555 The PD is connected](#)

3.3.14 ALM-303046663 The PD classes are invalid

Description

POE/4/PDINVALIDCLASS: OID [OID] PD with invalid IEEE class and power denied.
(IfIndex=[INTEGER], Interface="[OCTET"])

The system detects that the PD class is invalid.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046663	Warning	Communication alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
IfIndex	Indicates the interface index.
Interface	Indicates the interface name.

Impact on the System

Services are not affected.

Possible Causes

Cause 1:

The PD may not comply with standards, whereas the switch supports 802.3af and 802.3at. In this case, the PD class cannot be identified by the switch.

Cause 2:

The PD hardware is faulty.

Cause 3:

The PoE chip of the device is faulty.

Procedure

Step 1 Run the **poe legacy enable** command on the interface to enable compatibility detection and then check whether the alarm is cleared.

If so, the alarm handling ends.

If not, go to step 2.

Step 2 Replace the PD with a standard PD and then check whether the alarm is cleared.

If so, the alarm handling ends.

If not, collect alarm information and configuration information, and then contact technical support personnel.

----End

Related Information

None

3.3.15 ALM-303046662 The PD classes exceed the threshold

Description

POE/4/PDCLASSOVERCURRENT: OID [OID] has detected a classification overcurrent PD and power denied.(IfIndex=[INTEGER], Interface="[OCTET]")

The system detects that overcurrent occurs during PD classification.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046662	Warning	Communication alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
IfIndex	Indicates the interface index.
Interface	Indicates the interface name.

Impact on the System

Services are not affected.

Possible Causes

The PD does not comply with standards.

Procedure

Step 1 Run the **poe high-inrush enable slot *slot-id*** command in the system view to allow high inrush current during power-on and then check whether the alarm is cleared.

If so, the alarm handling ends.

If not, go to step 2.

Step 2 Replace the PD with a standard PD and then check whether the alarm is cleared.

If so, the alarm handling ends.

If not, collect alarm information and configuration information, and then contact technical support personnel.

----End

Related Information

None

3.3.16 ALM-303046674 The Local Priority of the PD Is Different from the Priority Obtained Through LLDP

Description

POE/4/PDPRIDIFF: OID [OID] priority inconsistent.(IfIndex=[INTEGER], Interface="[OCTET]", PortPriority=[INTEGER], PDPriority=[INTEGER])

The interface priority is different from the PD priority.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046674	Warning	Quality of service alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
IfIndex	Indicates the interface index.
Interface	Indicates the interface name.
PortPriority	Indicates the interface priority.
PDPriority	Indicates the PD priority.

Impact on the System

Services are not affected.

Possible Causes

The interface priority is low, whereas the PD priority is high.

Procedure

Run the **poe priority** command to change the interface priority to be higher than the PD priority.

Related Information

None

3.3.17 ALM-303046673 The Power Consumption of the PSE Exceeds the Upper Limit

Description

POE/4/PWRUTITHRESH: OID [OID] PSE is overdrawing power.(SlotID=[I NTEGER], ConsumingPower=[INTEGER], PowerThreshold=[INTEGER])

The total PoE power consumption is greater than or equal to the alarm threshold.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046673	Warning	Communication alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
SlotID	Indicates the ID of the slot where the alarm is generated.
ConsumingPower	Indicates the current power consumption.
PowerThreshold	Indicates the power threshold.

Impact on the System

If the alarm persists, all the PDs may be powered off because of insufficient power supply.

Possible Causes

The total power consumption of all the PDs is greater than or equal to the alarm threshold.

Procedure

Plan the network according to the system power supply. Increase priorities of important devices to prevent their power from being preempted. If the alarm persists, power off some PDs to ensure system reliability.

Related Information

None

3.3.18 ALM-303046672 The PoE power module is abnormal

Description

POE/4/POEPWABSENT: OID [OID] POE Power is absent.(FrameID = [INTEGER], SlotID = [INTEGER])

An alarm is triggered when no PoE power supply on a PoE device is working properly.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046672	Warning	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
FrameID	Indicates the chassis ID of a device in a stack.
SlotID	Indicates the slot ID of the PoE power supply.

Impact on the System

Services are not affected.

Possible Causes

No PoE power supply on the PoE device is working properly.

Procedure

- Step 1** Run the **display device** command to check whether power modules of the **PWR** or **PWH** type are properly installed.

- If not, install a PoE power module. The alarm handling ends.
- If so, go to step 2.

Step 2 Run the **display poe information** command to check whether the power of the PoE power module is in the normal range.

- If so, collect alarm information and configuration information, and then contact technical support personnel.
- If not, replace this PoE power module.

----End

3.3.19 ALM-303046425 The link is disconnected

Description

IFNET/1/IF_LINKDOWN: OID [OID] Interface [interface-index] turned into DOWN state.(AdminStatus=[INTEGER],OperStatus=[INTEGER],InterfaceName=[OCTET])

The status of the link protocol on the interface became Down.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046425	Critical	other(1)

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
interface-index	Indicates the interface index.
AdminStatus	Indicates the admin status, which means whether the interface has been disabled. • 1: undo shutdown • 2: shutdown
OperStatus	Indicates the operating status, which means the link layer protocol status of the interface. • 1: Up • 2: Down
InterfaceName	Indicates the interface name.

Impact on the System

The interface cannot forward packets normally.

Possible Causes

Cause 1:

The interface became Down and the link was disconnected.

Cause 2:

The VLANIF interface is deleted.

Procedure

- Step 1** If the VLANIF interface is deleted, this trap message is informational only. No action is required, go to Step 7.
- Step 2** Run the **display this** command in the interface view to check whether interfaces on both ends are shut down.
- If so, go to Step 3.
 - If not, go to Step 4.
- Step 3** Run the **undo shutdown** command in the interface view to check whether the alarm is cleared.
- If so, go to Step 7.
 - If not, go to Step 4.
- Step 4** Check whether the cable and optical module are loosened or dropped.
- If so, go to Step 6.
 - If not, go to Step 5.
- Step 5** Connect the physical link correctly and then check whether the alarm is cleared.
- If so, go to Step 7.
 - If not, go to Step 6.
- Step 6** Collect alarm information and configuration information, and then contact technical support personnel.
- Step 7** End.
- End

Related Information

None

3.3.20 ALM-3276800000 Indicates that SFP is not certified 136192

Description

SRM/3/SFP_EXCEPTION: OID [OID] Optical module exception, SFP is not certified.
(EntityPhysicalIndex=[INTEGER], BaseTrapSeverity=[INTEGER],

BaseTrapProbableCause=[INTEGER], BaseTrapEventType=[INTEGER],
EntPhysicalContainedIn=[INTEGER], EntPhysicalName=[OCTET],
RelativeResource=[OCTET], ReasonDescription=[OCTET])

An optical module installed on the device is not a Huawei-customized optical module.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800000	Minor	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
EntityPhysicalIndex	Indicates a physical entity index.
BaseTrapSeverity	Indicates the alarm severity.
BaseTrapProbableCause	Indicates the error code of the alarm.
BaseTrapEventType	Indicates the event type.
EntPhysicalContainedIn	Indicates contained physical entity code.
EntPhysicalName	Indicates the physical entity name.
RelativeResource	Indicates the entity-related resources.
ReasonDescription	Describes reason of the fault.

Impact on the System

If this optical module was delivered from Huawei early, this alarm does not affect the system. If not, the optical module may not work normally.

Possible Causes

The optical module is not a Huawei-customized optical module. Vendor information of the early delivered Huawei optical module is not recorded.

Procedure

- If this optical module was delivered from Huawei earlier, run the **transceiver phony-alarm-disable** command to disable the alarm function for non-Huawei customized optical modules.

- If this optical module is not delivered from Huawei or is not customized for Huawei, replace it with a Huawei-customized optical module.

Related Information

None

3.3.21 ALM-3276800001 Indicates that temperature exceeded the upper pre-alarm limit

Description

SRM/3/TEMPRISINGALARM: OID [OID] temperature over high threshold .
(EntityPhysicalIndex=[INTEGER1],
BaseThresholdEntry_entPhysicalIndex=[INTEGER2],
BaseThresholdEntry_hwBaseThresholdType=[INTEGER3],
BaseThresholdEntry_hwBaseThresholdIndex=[INTEGER4],
BaseTrapSeverity=[INTEGER5], BaseTrapProbableCause=[INTEGER6],
BaseTrapEventType=[INTEGER7], EntPhysicalName=[OCTET],
BaseThresholdValue=[INTEGER8], BaseThresholdUnit=[INTEGER9],
BaseThresholdHighWarning=[INTEGER10],
BaseThresholdHighCritical=[INTEGER11])

The temperature exceeded the upper threshold.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800001	Minor	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
EntityPhysicalIndex	Entity index.
BaseThresholdEntry_entPhysicalIndex	Index of the entity causing this temperature alarm.
BaseThresholdEntry_hwBaseThreshold-Type	Type of the detected entity (The value 1 indicates the temperature sensor of a certain type that is adopted by the S-switch.)
BaseThresholdEn-try_hwBaseThresholdIndex	Index of the temperature sensor (The value begins from 1.)
BaseTrapSeverity	Severity code.

Name	Meaning
BaseTrapProbableCause	Error code.
BaseTrapEventType	Code of the event type.
EntPhysicalName	Entity name.
BaseThresholdValue	Current temperature.
BaseThresholdUnit	Unit of the temperature.
BaseThresholdLowWarning	Upper threshold of the temperature.
BaseThresholdLowWarning	Major upper threshold of the temperature.

Impact on the System

When the temperature exceeds the upper threshold, the switch may not work properly and packet loss may occur. Or more seriously, the system may not respond or reset abnormally.

Possible Causes

- The chassis is not ventilated well, which causes heat unable to be dissipated.
- The ambient temperature is high.
- There are not enough fans in the switch.
- One or more fans in the switch have failed.
- The upper threshold of the temperature is too low.

Procedure

Step 1 Clean the air vents and check whether the alarm is cleared.

(1) If so, go to step 13.

(2) If not, go to step 2.

Step 2 Check whether the ambient temperature is high.

(1) If so, go to step 3.

(2) If not, go to step 4.

Step 3 Lower the temperature in the equipment room, and then go to step 4.

Step 4 Check whether all the fans are present and working normally.

(1) If so, go to step 6.

(2) If not, go to step 5.

Step 5 Install more fans in the switch, and then go to step 6.

- Step 6** Run the **display fan** command to check the status of fans and determine whether any fan is faulty.
- (1) If so, go to step 7.
 - (2) If not, go to step 8.
- Step 7** Replace the faulty fan, and then go to step 8.
- Step 8** After the switch has been running for a period of time, run the **display temperature all** command to check whether temperature of the switch is still high.
- (1) If so, go to step 9.
 - (2) If not, go to step 13.
- Step 9** Check whether the upper threshold of the temperature is too low.
- (1) If so, go to step 10.
 - (2) If not, go to step 12.
- Step 10** Run the **temperature threshold slot *slotid* lower-limit *lower* upper-limit *upper*** command to set a higher upper threshold of the temperature.
- Step 11** After the switch has been running for a period of time, run the **display temperature all** command to check whether temperature of the switch is still high.
- (1) If so, go to step 12.
 - (2) If not, go to step 13.
- Step 12** Contact technical support personnel.
- Step 13** End.
- End

Related Information

None

3.3.22 ALM-3276800002 Indicates that temperature exceeded the lower pre-alarm limit

Description

SRM/3/TEMPFALLINGALARM: OID [OID] temperature below minor threshold .
(EntityPhysicalIndex=[INTEGER1],
BaseThresholdEntry_entPhysicalIndex=[INTEGER2],
BaseThresholdEntry_hwBaseThresholdType=[INTEGER3],
BaseThresholdEntry_hwBaseThresholdIndex=[INTEGER4],
BaseTrapSeverity=[INTEGER5], BaseTrapProbableCause=[INTEGER6],
BaseTrapEventType=[INTEGER7], EntPhysicalName=[OCTET],
BaseThresholdValue=[INTEGER8], BaseThresholdUnit=[INTEGER9],
BaseThresholdLowCritical=[INTEGER10],
BaseThresholdLowWarning=[INTEGER11])

This alarm was generated when the temperature was lower than the lower threshold.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800002	Minor	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
EntityPhysicalIndex	Entity index.
BaseThresholdEntry_entPhysicalIndex	Index of the entity causing this temperature alarm.
BaseThresholdEntry_hwBaseThreshold-Type	Type of the detected entity (The value 1 indicates the temperature sensor of a certain type that is adopted by the S-switch.)
BaseThresholdEntry_hwBaseThresholdIndex	Index of the temperature sensor (The value begins from 1.)
BaseTrapSeverity	Severity code.
BaseTrapProbableCause	Error code.
BaseTrapEventType	Code of the event type.
EntPhysicalName	Entity name.
BaseThresholdValue	Current temperature.
BaseThresholdUnit	Unit of the temperature.
BaseThresholdLowCritical	Major lower threshold of the temperature.
BaseThresholdLowWarning	Lower threshold of the temperature.

Impact on the System

After the temperature exceeds the lower threshold, the device may fail to work normally. That is, packet loss may occur or even more seriously, the device may be suspended or abnormally reset.

Possible Causes

1. The lower threshold of the temperature was too high.
2. The ambient temperature was too low.

Procedure

- Step 1** Run the **display temperature { all | slot *slot-id* }** command to check whether the ambient temperature is too low.
- If so, increase the ambient temperature by turning up the air-conditioner.
 - If not, go to step 2.
- Step 2** Run the **display temperature { all | slot *slot-id* }** command to check whether the set lower threshold of the temperature is too high.
- If so, set the lower threshold of the temperature to a proper value. It is recommended that you run the **undo temperature threshold unit *unit-id*** command to restore the lower threshold to the default value.
 - If not, the alarm handling ends.

----End

3.3.23 ALM-3276800003 Indicates that chip exception 67590

Description

SRM/3/ENTITYINVALID: OID [OID] temperature chip exception.
(EntityPhysicalIndex[INTEGER1], BaseTrapSeverity=[INTEGER2],
BaseTrapProbableCause=[INTEGER3], BaseTrapEventType=[INTEGER4],
EntPhysicalContainedIn=[INTEGER5], EntPhysicalName=[OCTET1],
RelativeResource=[OCTET2], ReasonDescription=[OCTET3])

This alarm was generated when the chip was detected abnormal.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800003	Minor	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
EntityPhysicalIndex	Entity index.
BaseTrapSeverity	Severity code.

Name	Meaning
BaseTrapProbableCause	Error code.
BaseTrapEventType	Code of the event type.
EntPhysicalContainedIn	Entity code.
EntPhysicalName	Entity name.
RelativeResource	Name of the affected component.
ReasonDescription	Fault description.

Impact on the System

The temperature of the board cannot be obtained. As a result, the fan module cannot automatically adjust the rotational speed according to the temperature of the board. The fan module thus keeps working at the full rotational speed with too much noise. The services, however, are not affected.

Possible Causes

The IIC bus was faulty.

Procedure

- Step 1** Run the **display temperature { all | slot *slot-id* }** command to check whether a fault occurs on the temperature sensor due to the faulty IIC bus.
- (1) If the character string "Read Temperature Fail" is displayed in the query result, it indicates that the IIC bus is faulty. In this case, you need to replace the device.
- (2) If the character string "Read Temperature Fail" is not displayed in the query result, it indicates that the fault on the IIC bus is rectified. In this case, you need to go to Step 2.
- Step 2** End.
- End

Related Information

None

3.3.24 ALM-3276800004 A Fan Module Does Not Work Properly

Description

SRM/3/ENTITYINVALID: OID [OID] Fan loss. (EntityPhysicalIndex[INTEGER1], BaseTrapSeverity=[INTEGER2], BaseTrapProbableCause=[INTEGER3], BaseTrapEventType=[INTEGER4], EntPhysicalContainedIn=[INTEGER5],

EntPhysicalName=[OCTET1], RelativeResource=[OCTET2],
ReasonDescription=[OCTET3])

A fan module does not work normally.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800004	Minor	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
EntityPhysicalIndex	Entity index.
BaseTrapSeverity	Severity code.
BaseTrapProbableCause	Error Code.
BaseTrapEventType	Code of the event type.
EntPhysicalContainedIn	Entity code.
EntPhysicalName	Entity name.
RelativeResource	Name of the affected component.
ReasonDescription	Fault description.

Impact on the System

When the fan module fails to work normally, card temperature will increase, which may result in packet loss or even more seriously, failure of the switch to respond or unexpected restart.

Possible Causes

The cable of the fan module was connected loosely or the fan hardware was faulty.

Procedure

Step 1 Remove and insert the fan module and check whether the fault is rectified.

(1) If the fault persists, the fan hardware is faulty. In this case, replace the fan module.

(2) If the fault is rectified, go to Step 2.

Step 2 End.
----End

Related Information

None

3.3.25 ALM-3276800005 Indicates that PHY chip abnormal 67861

Description

SRM/3/ENTITYINVALID: OID [OID] PHY chip abnormal.
(EntityPhysicalIndex[INTEGER1], BaseTrapSeverity=[INTEGER2],
BaseTrapProbableCause=[INTEGER3], BaseTrapEventType=[INTEGER4],
EntPhysicalContainedIn=[INTEGER5], EntPhysicalName=[OCTET1],
RelativeResource=[OCTET2], ReasonDescription=[OCTET3])

This alarm was generated when the chip was detected abnormal.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800005	Minor	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
EntityPhysicalIndex	Entity index.
BaseTrapSeverity	Severity code.
BaseTrapProbableCause	Error code.
BaseTrapEventType	Code of the event type.
EntPhysicalContainedIn	Entity code.
EntPhysicalName	Entity name.
RelativeResource	Name of the affected component.
ReasonDescription	Fault description.

Impact on the System

The services on the interface corresponding to the faulty PHY chip are interrupted.

Possible Causes

The PHY chip was faulty.

Procedure

- Step 1** If the interface corresponding to the faulty PHY chip is Up, the device automatically resets. Then, you need to check whether the interface sends and receives packets normally.
- (1) If not, it indicates that the PHY chip is faulty. In this case, you need to replace the device.
 - (2) If so, go to Step 4.
- Step 2** If the interface corresponding to the faulty PHY chip is Down, the device does not reset automatically.
- (1) If you do not use the interface, no action is required.
 - (2) If you need to use the interface, go to Step 3.
- Step 3** Run the **reboot** command to reset the device, and then check whether the interface sends and receives packets normally.
- (1) If not, it indicates that the PHY chip is faulty. In this case, you need to replace the device.
 - (2) If so, go to Step 4.
- Step 4** End.
- End

Related Information

None

3.3.26 ALM-3276800006 Indicates that Optical module Tx power is too low

Description

SRM/3/TXPOWER_EXCEEDMINOR: OID [OID] Optical module exception, Tx power is too low. (EntityPhysicalIndex=[INTEGER], BaseTrapSeverity=[INTEGER], BaseTrapProbableCause=[INTEGER], BaseTrapEventType=[INTEGER], EntPhysicalContainedIn=[INTEGER], EntPhysicalName=[OCTET], RelativeResource=[OCTET], ReasonDescription=[OCTET])

The transmit power of an optical module is too low.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800006	Minor	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
Index	Indicates the index.
EntityPhysicalIndex	Indicates the index of the physical entity.
PhysicalName	Indicates the name of the physical entity.
EntityTrapFaultID	Indicates the error code.
EntityTrapReasonDescr	Indicates the description of the alarm cause.

Impact on the System

This alarm does not affect system operating if the interface on which the optical module is installed works properly.

Possible Causes

The transmit power of the optical module is too low.

Procedure

- Step 1** Run the **display transceiver slot *slot-id* verbose** command in the system view to check whether the transmit power **Tx Power** of the optical module is within the allowed range.
 - If so, services are not affected. Collect alarms, logs, and configurations and contact technical support personnel.
 - If not, go to step 2.
- Step 2** Check whether the transmit power lower threshold of the optical module is within the acceptable range.
 - If so, run the **transceiver diagnosis threshold tx-power** command to change the transmit power lower threshold of the optical module. The alarm handling ends.
 - If not, go to step 3.

- Step 3** Replace the optical module, and check whether the alarm is cleared.
- If so, the alarm handling ends.
 - If not, collect alarms, logs, and configurations, and contact technical support personnel.
- End

Related Information

None

3.3.27 ALM-3276800007 Indicates that Optical module Rx power is too low

Description

SRM/3/RXPOWER_EXCEEDMINOR: OID [OID] Optical module exception, Rx power is too low. (EntityPhysicalIndex=[INTEGER], BaseTrapSeverity=[INTEGER], BaseTrapProbableCause=[INTEGER], BaseTrapEventType=[INTEGER], EntPhysicalContainedIn=[INTEGER], EntPhysicalName=[OCTET], RelativeResource=[OCTET], ReasonDescription=[OCTET])

The receive power of an optical module is too low.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800007	Minor	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
Index	Indicates the index.
EntityPhysicalIndex	Indicates the index of the physical entity.
PhysicalName	Indicates the name of the physical entity.
EntityTrapFaultID	Indicates the error code.
EntityTrapReasonDescr	Indicates the description of the alarm cause.

Impact on the System

This alarm does not affect system operating if the interface on which the optical module is installed works properly.

Possible Causes

The receive power of the optical module was too low.

Procedure

- Step 1** Run the **display transceiver slot *slot-id* verbose** command in the system view to check whether the receive power **Rx Power** of the local interface is within the acceptable range.
- If so, collect alarms, logs, and configurations, and contact technical support personnel.
 - If not, go to step 2.
- Step 2** Check whether the receive power of the optical module is within a usable range.
- If so, run the **transceiver diagnosis threshold rx-power** command to change the receive power lower threshold of the optical module. The alarm handling ends.
 - If not, go to step 3.
- Step 3** Check whether the peer port is physically Up and whether there is no alarm indicating that the transmit power is too low.
- If so, perform an external loopback test on the interface. If the interface is in Up state, perform loopback tests on the nodes along the transmission path to locate the failure point or link. Then check whether the alarm is cleared. If not, go to 4.
 - If not, go to step 4.
- Step 4** Check whether the peer port is physically Down and a corresponding alarm is generated, rectify the fault on the peer port.
- If so, repair the peer port. Check whether the alarm is cleared. If not, go to step 5.
 - If not, go to step 5.
- Step 5** Test whether the fiber is working normally.
- If so, replace the fiber and check whether the alarm is cleared. If not, go to step 6.
 - If not, go to step 6.
- Step 6** Replace the optical module of the local port and check whether the alarm is cleared.
- If so, the alarm handling ends.
 - If not, go to step 7.
- Step 7** Collect alarms, logs, and configurations, and contact technical support personnel.

----End

Related Information

None

3.3.28 ALM-3276800008 Indicates that power loss 67967

Description

SRM/3/POWERABSENT: OID [OID] Power is absent.
(EntityPhysicalIndex=[INTEGER], BaseTrapSeverity=[INTEGER],
BaseTrapProbableCause=[INTEGER], BaseTrapEventType=[INTEGER],
EntPhysicalContainedIn=[INTEGER], EntPhysicalName=[OCTET],
RelativeResource=[OCTET], ReasonDescription=[OCTET])

The power supply unit of a device is removed.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800008	Minor	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
EntityPhysicalIndex	Indicates the index of the physical entity.
BaseTrapSeverity	Indicates the severity level.
BaseTrapProbableCause	Indicates the error code: 67967.
BaseTrapEventType	Indicates the event type.
EntPhysicalContainedIn	Indicates the code of the physical entity.
EntPhysicalName	Indicates the name of the physical entity.
RelativeResource	Indicates the sub-entity.
ReasonDescription	Indicates the fault description.

Impact on the System

If the device uses only one power supply, the device is powered off after the power supply is removed and services are interrupted.

Possible Causes

- The internal power module encounters a power failure.
- The internal power module is removed.
- The lead-acid battery is removed.

Procedure

Install the power supply.

Related Information

None

3.3.29 ALM-3276800009 Indicates that power abnormal 67966

Description

SRM/1/POWERFAULT: OID [OID] Power is abnormal.
(EntityPhysicalIndex=[INTEGER], BaseTrapSeverity=[INTEGER],
BaseTrapProbableCause=[INTEGER], BaseTrapEventType=[INTEGER],
EntPhysicalContainedIn=[INTEGER], EntPhysicalName=[OCTET],
RelativeResource=[OCTET], ReasonDescription=[OCTET])

The power module is faulty.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800009	Critical	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
EntityPhysicalIndex	Indicates the index of the physical entity.
BaseTrapSeverity	Indicates the severity level.
BaseTrapProbableCause	Indicates the error code.
BaseTrapEventType	Indicates the event type.
EntPhysicalContainedIn	Indicates the code of the physical entity.

Name	Meaning
EntPhysicalName	Indicates the name of the physical entity.
RelativeResource	Indicates the sub-entity.
ReasonDescription	Indicates the fault description.

Impact on the System

The device cannot receive sufficient power supply.

Possible Causes

- The power module is powered off.
- The power module does not load the correct electronic label.

Procedure

Power on the power module. If the alarm is not cleared, replace the power module.

Related Information

None

3.3.30 ALM-3276800010 Indicates that Tx Power Exceed Major

Description

SRM/3/TXPOWER_EXCEED: OID [OID] Optical module exception, Tx power is too high. (EntityPhysicalIndex=[INTEGER], BaseTrapSeverity=[INTEGER], BaseTrapProbableCause=[INTEGER], BaseTrapEventType=[INTEGER], EntPhysicalContainedIn=[INTEGER], EntPhysicalName=[OCTET], RelativeResource=[OCTET], ReasonDescription=[OCTET])

The transmit power of an optical module is too high.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800010	Minor	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
Index	Indicates the index.
EntityPhysicalIndex	Indicates the index of the physical entity.
PhysicalName	Indicates the name of the physical entity.
EntityTrapFaultID	Indicates the error code.
EntityTrapReasonDescr	Indicates the description of the alarm cause.

Impact on the System

This alarm does not affect system operating if the interface on which the optical module is installed works properly.

Possible Causes

The transmit power of the optical module is too high.

Procedure

- Step 1** Run the **display transceiver slot *slot-id* verbose** command in the system view to check whether the transmit power **Tx Power** of the optical module is within the allowed range.
- If so, services are not affected. Collect alarms, logs, and configurations and contact technical support personnel.
 - If not, go to step 2.
- Step 2** Check whether the transmit power upper threshold of the optical module is within the acceptable range.
- If so, run the **transceiver diagnosis threshold tx-power** command to change the transmit power upper threshold of the optical module. The alarm handling ends.
 - If not, go to step 3.
- Step 3** Use an optical attenuator to reduce the transmit power of the optical module to the acceptable range. Check whether the alarm is cleared.
- If so, the alarm handling ends.
 - If not, go to step 4.
- Step 4** Replace the optical module, and check whether the alarm is cleared.

- If so, the alarm handling ends.
- If not, collect alarms, logs, and configurations, and contact technical support personnel.

----End

Related Information

None

3.3.31 ALM-3276800011 Indicates that Rx Power Exceed Major

Description

SRM/3/RXPOWER_EXCEEDMAJOR: OID [OID] Optical module exception, Rx power is too high. (EntityPhysicalIndex=[INTEGER], BaseTrapSeverity=[INTEGER], BaseTrapProbableCause=[INTEGER], BaseTrapEventType=[INTEGER], EntPhysicalContainedIn=[INTEGER], EntPhysicalName=[OCTET], RelativeResource=[OCTET], ReasonDescription=[OCTET])

The receive power of an optical module is too high.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800011	Minor	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
Index	Indicates the index.
EntityPhysicalIndex	Indicates the index of the physical entity.
PhysicalName	Indicates the name of the physical entity.
EntityTrapFaultID	Indicates the error code.
136195	Indicates that the receive power of the optical module is too high.
EntityTrapReasonDescr	Indicates the description of the alarm cause.

Impact on the System

This alarm does not affect system operating if the interface on which the optical module is installed works properly.

Possible Causes

The receive power is too high.

Procedure

- Step 1** Run the **display transceiver slot *slot-id* verbose** command in the system view to check whether the receive power **Rx Power** of the optical module is within the allowed range.
- If so, collect alarms, logs, and configurations, and contact technical support personnel.
 - If not, go to step 2.
- Step 2** Check whether the receive power of the optical module is within a usable range.
- If so, run the **transceiver diagnosis threshold rx-power** command to change the receive power upper threshold of the optical module. The alarm handling ends.
 - If not, go to step 3.
- Step 3** Check whether an alarm is generated for high transmit power on the peer optical module. If so, rectify the peer optical module fault first.
- Step 4** Check whether the peer optical module and the local optical module are of the same type. If not, replace the local optical module with a new one to ensure they are of the same type.
- Step 5** Add -5 dBm (recommended) attenuators to the optical module.
- Step 6** If the problem persists after the preceding steps, collect alarms, logs, and configurations, and contact technical support personnel.

----End

Related Information

None

3.3.32 ALM-3276800012 Indicates that PHY abnormal 67958

Description

SRM/3/ENTITYINVALID: OID [OID] PHY is abnormal.
(EntityPhysicalIndex=[INTEGER], BaseTrapSeverity=[INTEGER],
BaseTrapProbableCause=[INTEGER], BaseTrapEventType=[INTEGER],
EntPhysicalContainedIn=[INTEGER], EntPhysicalName=[OCTET],
RelativeResource=[OCTET], ReasonDescription=[OCTET])

The PHY is faulty.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800012	Minor	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
EntityPhysicalIndex	Indicates a physical entity index.
BaseTrapSeverity	Indicates the alarm severity.
BaseTrapProbableCause	Indicates the error code of the alarm.
BaseTrapEventType	Indicates the event type.
EntPhysicalContainedIn	Indicates contained physical entity code.
EntPhysicalName	Indicates the physical entity name.
RelativeResource	Indicates a sub-entity.
ReasonDescription	Describes reason of the fault.

Impact on the System

The interface specified in the alarm cannot send or receive packets. The RUN indicator of the device is off, and the Alarm indicator is steady red.

Possible Causes

The PHY hardware component became faulty.

Procedure

Use a normally running interface to replace the faulty interface, and reconfigure service parameters on this interface.

Related Information

None

3.3.33 ALM-3276800013 Indicates that LAN Switch abnormal 67962

Description

SRM/3/ENTITYINVALID: OID [OID] Switch Chip is abnormal.
(EntityPhysicalIndex=[INTEGER], BaseTrapSeverity=[INTEGER],
BaseTrapProbableCause=[INTEGER], BaseTrapEventType=[INTEGER],
EntPhysicalContainedIn=[INTEGER], EntPhysicalName=[OCTET],
RelativeResource=[OCTET], ReasonDescription=[OCTET])

The switching chip on a card has failed.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800013	Minor	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
EntityPhysicalIndex	Indicates a physical entity index.
BaseTrapSeverity	Indicates the alarm severity.
BaseTrapProbableCause	Indicates the error code of the alarm.
BaseTrapEventType	Indicates the event type.
EntPhysicalContainedIn	Indicates contained physical entity code.
EntPhysicalName	Indicates the physical entity name.
RelativeResource	Indicates a sub-entity.
ReasonDescription	Describes reason of the fault.

Impact on the System

The card is reset.

Possible Causes

A hardware fault has occurred.

Procedure

Contact technical support personnel.

Related Information

None

3.3.34 ALM-3276800014 MP reached AC through the Ethernet port notify

Description

WLAN/4/MP_JOINED_ON_ETHERNET:OID [OID] MP reached AC through the Ethernet port, and this MP doesn't setup mesh link in avoid of loopback. (APMAC=[OPAQUE], APName=[STRING], APID=[INTEGER])

An MP goes online through an Ethernet interface.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800014	Warning	Communication alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
APMAC	Indicates the MAC address of an AP.
APName	Indicates the AP name.
APID	Indicates the AP ID.

Impact on the System

None

Possible Causes

An MP goes online through an Ethernet interface.

Procedure

Step 1 This alarm is informational only, and no action is required.

----End

Related Information

None

3.3.35 ALM-3276800015 Indicates that CPLD Check abnormal 67963

Description

SRM/3/ENTITYINVALID: OID [OID] CPLD is abnormal.
(EntityPhysicalIndex=[INTEGER], BaseTrapSeverity=[INTEGER], BaseTrapProbableCause=[INTEGER], BaseTrapEventType=[INTEGER], EntPhysicalContainedIn=[INTEGER], EntPhysicalName=[OCTET], RelativeResource=[OCTET], ReasonDescription=[OCTET])

The complex programmable logical device (CPLD) on a card has failed.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800015	Minor	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
EntityPhysicalIndex	Indicates a physical entity index.
BaseTrapSeverity	Indicates the alarm severity.
BaseTrapProbableCause	Indicates the error code of the alarm.
BaseTrapEventType	Indicates the event type.
EntPhysicalContainedIn	Indicates contained physical entity code.
EntPhysicalName	Indicates the physical entity name.
RelativeResource	Indicates a sub-entity.
ReasonDescription	Describes reason of the fault.

Impact on the System

The card is reset.

Possible Causes

A hardware fault has occurred.

Procedure

Contact technical support personnel.

Related Information

None

3.3.36 ALM-3276800016 MPP joins AC through the air notify

Description

WLAN/4/MPP_JOINED_ON_AIR:OID [oid] MPP can't reach AC through the Ethernet port,so this MPP joins AC through the air,changes itself to MP,and forbid traffic on the Ethernet port in avoid of loopback. (APMAC=[OPAQUE], APName=[STRING], APID=[INTEGER])

An MPP changes to an MP and goes online through an air interface.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800016	Warning	Communication alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
APMAC	Indicates the MAC address of an AP.
APName	Indicates the AP name.
APID	Indicates the AP ID.

Impact on the System

None

Possible Causes

Due to a link fault, an MPP changes to an MP and goes online through an air interface.

Procedure

This alarm is informational only, and no action is required.

Related Information

None

3.3.37 ALM-3276800017 Indicates that FPGA Check abnormal 67964

Description

SRM/3/ENTITYINVALID: OID [OID] FPGA is abnormal.
(EntityPhysicalIndex=[INTEGER], BaseTrapSeverity=[INTEGER],
BaseTrapProbableCause=[INTEGER], BaseTrapEventType=[INTEGER],
EntPhysicalContainedIn=[INTEGER], EntPhysicalName=[OCTET],
RelativeResource=[OCTET], ReasonDescription=[OCTET])

The field programmable gate array (FPGA) of a card has failed.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800017	Minor	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
EntityPhysicalIndex	Indicates a physical entity index.
BaseTrapSeverity	Indicates the alarm severity.
BaseTrapProbableCause	Indicates the error code of the alarm.
BaseTrapEventType	Indicates the event type.
EntPhysicalContainedIn	Indicates contained physical entity code.
EntPhysicalName	Indicates the physical entity name.
RelativeResource	Indicates a sub-entity.
ReasonDescription	Describes reason of the fault.

Impact on the System

If the fault persists, the card is reset.

Possible Causes

A hardware fault has occurred.

Procedure

Contact technical support personnel.

Related Information

None

3.3.38 ALM-3276800018 Indicates that USB abnormal 68072

Description

SRM/3/ENTITYINVALID: OID [OID] USB is abnormal.
(EntityPhysicalIndex=[INTEGER], BaseTrapSeverity=[INTEGER],
BaseTrapProbableCause=[INTEGER], BaseTrapEventType=[INTEGER],
EntPhysicalContainedIn=[INTEGER], EntPhysicalName=[OCTET],
RelativeResource=[OCTET], ReasonDescription=[OCTET])

The USB port has failed.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800018	Minor	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
EntityPhysicalIndex	Indicates a physical entity index.
BaseTrapSeverity	Indicates the alarm severity.
BaseTrapProbableCause	Indicates the error code of the alarm.
BaseTrapEventType	Indicates the event type.
EntPhysicalContainedIn	Indicates contained physical entity code.
EntPhysicalName	Indicates the physical entity name.

Name	Meaning
RelativeResource	Indicates a sub-entity.
ReasonDescription	Describes reason of the fault.

Impact on the System

The device cannot be upgraded using a USB flash drive.

Possible Causes

A hardware fault has occurred.

Procedure

Contact technical support personnel.

Related Information

None

3.3.39 ALM-3276800019 Indicates that USB 5v Power abnormal 68074

Description

SRM/4/USBPOWFAULT: OID [OID] USB 5v Power is abnormal.
(EntityPhysicalIndex=[INTEGER1], BaseTrapSeverity=[INTEGER2],
BaseTrapProbableCause=[INTEGER3], BaseTrapEventType=[INTEGER4],
EntPhysicalContainedIn=[INTEGER5], EntPhysicalName=[OCTET1],
RelativeResource=[OCTET2], ReasonDescription=[OCTET3])

USB 5 V power supply was faulty.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800019	Warning	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
EntityPhysicalIndex	Indicates the index of an entity.

Name	Meaning
BaseTrapSeverity	Indicates the alarm severity.
BaseTrapProbableCause	Indicates the possible causes of an alarm.
BaseTrapEventType	Indicates the type of an alarm.
EntPhysicalContainedIn	Indicates the index of a parent entity.
EntPhysicalName	Indicates the name of an entity.
RelativeResource	Indicates the entity-related resources.
ReasonDescription	Indicates the reason description of an alarm.

Impact on the System

The USB flash drive cannot work properly.

Possible Causes

The USB power supply has failed.

Procedure

- If USB-based deployment is not required, ignore the alarm.
- If USB-based deployment is required, replace the device.

Related Information

None

3.3.40 ALM-3276800020 Indicates that I2C abnormal 68080

Description

SRM/3/ENTITYINVALID: OID [OID] I2C is abnormal.
(EntityPhysicalIndex=[INTEGER1], BaseTrapSeverity=[INTEGER2],
BaseTrapProbableCause=[INTEGER3], BaseTrapEventType=[INTEGER4],
EntPhysicalContainedIn=[INTEGER5], EntPhysicalName=[OCTET1],
RelativeResource=[OCTET2], ReasonDescription=[OCTET3])

The I2C was faulty.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800020	Minor	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
EntityPhysicalIndex	Indicates the index of an entity.
BaseTrapSeverity	Indicates the alarm severity.
BaseTrapProbableCause	Indicates the possible causes of an alarm.
BaseTrapEventType	Indicates the type of an alarm.
EntPhysicalContainedIn	Indicates the index of a parent entity.
EntPhysicalName	Indicates the name of an entity.
RelativeResource	Indicates the entity-related resources.
ReasonDescription	Indicates the reason description of an alarm.

Impact on the System

One or more interfaces do not work normally.

Possible Causes

The I2C has failed.

Procedure

Step 1 Switch services from the interfaces affected by the I2C failure to interfaces that can work normally. If you still want to use an affected interface, rectify the I2C fault, and then run the **clear configuration interface** *interface-type interface-num* command to clear interface configuration and reconfigure the interface.

Step 2 If the fault cannot be rectified and services cannot be switched to normal interfaces, replace the device.

----End

Related Information

None

3.3.41 ALM-3276800021 Indicates that RTC abnormal 68082

Description

SRM/3/ENTITYINVALID: OID [OID] RTC abnormal.
(EntityPhysicalIndex=[INTEGER1], BaseTrapSeverity=[INTEGER2],

BaseTrapProbableCause=[INTEGER3], BaseTrapEventType=[INTEGER4],
EntPhysicalContainedIn=[INTEGER5], EntPhysicalName=[OCTET1],
RelativeResource=[OCTET2], ReasonDescription=[OCTET3])

The RTC was faulty.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800021	Minor	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
EntityPhysicalIndex	Indicates the index of an entity.
BaseTrapSeverity	Indicates the alarm severity.
BaseTrapProbableCause	Indicates the possible causes of an alarm.
BaseTrapEventType	Indicates the type of an alarm.
EntPhysicalContainedIn	Indicates the index of a parent entity.
EntPhysicalName	Indicates the name of an entity.
RelativeResource	Indicates the entity-related resources.
ReasonDescription	Indicates the reason description of an alarm.

Impact on the System

The RTC function does not work. After the device is power recycled, the system time will restore to the default value, affecting system time-based services, such as ACLs with time ranges configured.

Possible Causes

The RTC module failed or the RTC battery power was low.

Procedure

Contact technical support personnel.

Related Information

None

3.3.42 ALM-3276800022 Indicates that optical module power abnormal

Description

SRM/3/OPTPWABNORMAL: OID [OID] Optical module power is abnormal.
(EntityPhysicalIndex=[INTEGER], BaseTrapSeverity=[INTEGER], BaseTrapProbableCause=[INTEGER], BaseTrapEventType=[INTEGER], EntPhysicalContainedIn=[INTEGER], EntPhysicalName="[OCTET]", RelativeResource="[OCTET]", ReasonDescription="[OCTET]")

An alarm is generated when the transmit or receive power of an optical module is out of the allowed range.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800022	Minor	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
EntityPhysicalIndex	Indicates the physical index.
BaseTrapSeverity	Indicates the alarm severity.
BaseTrapProbableCause	Indicates the possible causes of the alarm.
BaseTrapEventType	Indicates the alarm type.
EntPhysicalContainedIn	Indicates the parent index of the entity.
EntPhysicalName	Indicates the name of the entity.
RelativeResource	Indicates the part related to the alarm.
ReasonDescription	Indicates the description of the alarm cause.

Impact on the System

This alarm does not affect system operating if the interface on which the optical module is installed works properly.

Possible Causes

The **ReasonDescription** parameter in the alarm describes the cause for the abnormal optical power.

- Cause 1: The transmit power of the optical module exceeds the maximum value. The **ReasonDescription** parameter description includes the following: Tx power is too high.
- Cause 2: The transmit power of the optical module falls below the minimum value. The **ReasonDescription** parameter description includes the following: Tx power is too low.
- Cause 3: The receive power of the optical module exceeds the maximum value. The **ReasonDescription** parameter description includes the following: Rx power is too high.
- Cause 4: The receive power of the optical module falls below the minimum value. The **ReasonDescription** parameter description includes the following: Rx power is too low.

NOTE

If the interface is in shutdown, errordown, or loopback state, this alarm is not generated when the transmit power falls below the minimum value. When a link fault occurs, the interface enabled with the ALS function sends LOS signals. This alarm is not generated when the transmit power or the receive power falls below the minimum value.

Procedure

- Step 1** Run the **display transceiver verbose** command to check the power of the optical module.
- Step 2** Check whether the interface status and data forwarding are normal.
- If so, run the **transceiver diagnosis threshold rx-power** command to change the receive power alarm threshold of the optical module or run the **transceiver diagnosis threshold tx-power** command to change the transmit power alarm threshold of the optical module.
 - If not, replace the optical module or collect alarm information and configuration information, and then contact technical support personnel.

----End

Related Information

None

3.3.42.1 ALM-3276800022 Indicates that optical module power abnormal 136193

Description

SRM/3/TXPOWER_EXCEEDMAJOR: OID [OID] Optical module exception, Tx power is too high. (EntityPhysicalIndex=[INTEGER], BaseTrapSeverity=[INTEGER], BaseTrapProbableCause=[INTEGER], BaseTrapEventType=[INTEGER], EntPhysicalContainedIn=[INTEGER], EntPhysicalName=[OCTET], RelativeResource=[OCTET], ReasonDescription=[OCTET])

The transmit power of an optical module is too high.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800022	Minor	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
Index	Indicates the index.
EntityPhysicalIndex	Indicates the index of the physical entity.
PhysicalName	Indicates the name of the physical entity.
EntityTrapFaultID	Indicates the error code.
EntityTrapReasonDescr	Indicates the description of the alarm cause.

Impact on the System

This alarm does not affect system operating if the interface on which the optical module is installed works properly.

Possible Causes

The transmit power of the optical module is too high.

Procedure

- Step 1** Run the **display transceiver slot *slot-id* verbose** command in the system view to check whether the transmit power **Tx Power** of the optical module is within the allowed range.
- If so, services are not affected. Collect alarms, logs, and configurations and contact technical support personnel.
 - If not, go to step 2.
- Step 2** Check whether the transmit power upper threshold of the optical module is within the acceptable range.
- If so, run the **transceiver diagnosis threshold tx-power** command to change the transmit power upper threshold of the optical module. The alarm handling ends.
 - If not, go to step 3.
- Step 3** Use an optical attenuator to reduce the transmit power of the optical module to the acceptable range. Check whether the alarm is cleared.
- If so, the alarm handling ends.
 - If not, go to step 4.
- Step 4** Replace the optical module, and check whether the alarm is cleared.
- If so, the alarm handling ends.
 - If not, collect alarms, logs, and configurations, and contact technical support personnel.

----End

Related Information

None

3.3.42.2 ALM-3276800022 Indicates that optical module power abnormal 136194

Description

SRM/3/TXPOWER_EXCEEDMINOR: OID [OID] Optical module exception, Tx power is too low. (EntityPhysicalIndex=[INTEGER], BaseTrapSeverity=[INTEGER], BaseTrapProbableCause=[INTEGER], BaseTrapEventType=[INTEGER], EntPhysicalContainedIn=[INTEGER], EntPhysicalName=[OCTET], RelativeResource=[OCTET], ReasonDescription=[OCTET])

The transmit power of an optical module is too low.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800022	Minor	Equipment alarm

Parameters

Name	Meaning
oid	Indicates the MIB object ID of the alarm.
Index	Indicates the index.
EntityPhysicalIndex	Indicates the index of the physical entity.
PhysicalName	Indicates the name of the physical entity.
EntityTrapFaultID	Indicates the error code.
EntityTrapReasonDescr	Indicates the description of the alarm cause.

Impact on the System

This alarm does not affect system operating if the interface on which the optical module is installed works properly.

Possible Causes

The transmit power of the optical module is too low.

Procedure

- Step 1** Run the **display transceiver slot *slot-id* verbose** command in the system view to check whether the transmit power **Tx Power** of the optical module is within the allowed range.
- If so, services are not affected. Collect alarms, logs, and configurations and contact technical support personnel.
 - If not, go to step 2.
- Step 2** Check whether the transmit power lower threshold of the optical module is within the acceptable range.
- If so, run the **transceiver diagnosis threshold tx-power** command to change the transmit power lower threshold of the optical module. The alarm handling ends.
 - If not, go to step 3.
- Step 3** Replace the optical module, and check whether the alarm is cleared.
- If so, the alarm handling ends.
 - If not, collect alarms, logs, and configurations, and contact technical support personnel.

----End

Related Information

None

3.3.42.3 ALM-3276800022 Indicates that optical module power abnormal 136195

Description

SRM/3/RXPOWER_EXCEEDMAJOR: OID [OID] Optical module exception, Rx power is too high. (EntityPhysicalIndex=[INTEGER], BaseTrapSeverity=[INTEGER], BaseTrapProbableCause=[INTEGER], BaseTrapEventType=[INTEGER], EntPhysicalContainedIn=[INTEGER], EntPhysicalName=[OCTET], RelativeResource=[OCTET], ReasonDescription=[OCTET])

The receive power of an optical module is too high.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800022	Minor	Equipment alarm

Parameters

Name	Meaning
oid	Indicates the MIB object ID of the alarm.
Index	Indicates the index.
EntityPhysicalIndex	Indicates the index of the physical entity.
PhysicalName	Indicates the name of the physical entity.
EntityTrapFaultID	Indicates the error code.
136195	Indicates that the receive power of the optical module is too high.
EntityTrapReasonDescr	Indicates the description of the alarm cause.

Impact on the System

This alarm does not affect system operating if the interface on which the optical module is installed works properly.

Possible Causes

The receive power is too high.

Procedure

- Step 1** Run the **display transceiver slot *slot-id* verbose** command in the system view to check whether the receive power **Rx Power** of the optical module is within the allowed range.
- If so, collect alarms, logs, and configurations, and contact technical support personnel.
 - If not, go to step 2.
- Step 2** Check whether the receive power of the optical module is within a usable range.
- If so, run the **transceiver diagnosis threshold rx-power** command to change the receive power upper threshold of the optical module. The alarm handling ends.
 - If not, go to step 3.
- Step 3** Check whether an alarm is generated for high transmit power on the peer optical module. If so, rectify the peer optical module fault first.
- Step 4** Check whether the peer optical module and the local optical module are of the same type. If not, replace the local optical module with a new one to ensure they are of the same type.
- Step 5** Add -5 dBm (recommended) attenuators to the optical module.
- Step 6** If the problem persists after the preceding steps, collect alarms, logs, and configurations, and contact technical support personnel.

----End

Related Information

None

3.3.42.4 ALM-3276800022 Indicates that optical module power abnormal 136196

Description

SRM/3/RXPOWER_EXCEEDMINOR: OID [OID] Optical module exception, Rx power is too low. (EntityPhysicalIndex=[INTEGER], BaseTrapSeverity=[INTEGER], BaseTrapProbableCause=[INTEGER], BaseTrapEventType=[INTEGER], EntPhysicalContainedIn=[INTEGER], EntPhysicalName=[OCTET], RelativeResource=[OCTET], ReasonDescription=[OCTET])

The receive power of an optical module is too low.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800022	Minor	Equipment alarm

Parameters

Name	Meaning
oid	Indicates the MIB object ID of the alarm.
Index	Indicates the index.
EntityPhysicalIndex	Indicates the index of the physical entity.
PhysicalName	Indicates the name of the physical entity.
EntityTrapFaultID	Indicates the error code.
EntityTrapReasonDescr	Indicates the description of the alarm cause.

Impact on the System

This alarm does not affect system operating if the interface on which the optical module is installed works properly.

Possible Causes

The receive power of the optical module was too low.

Procedure

- Step 1** Run the **display transceiver slot *slot-id* verbose** command in the system view to check whether the receive power **Rx Power** of the local interface is within the acceptable range.
- If so, collect alarms, logs, and configurations, and contact technical support personnel.
 - If not, go to step 2.
- Step 2** Check whether the receive power of the optical module is within a usable range.
- If so, run the **transceiver diagnosis threshold rx-power** command to change the receive power lower threshold of the optical module. The alarm handling ends.
 - If not, go to step 3.

- Step 3** Check whether the peer port is physically Up and whether there is no alarm indicating that the transmit power is too low.
- If so, perform an external loopback test on the interface. If the interface is in Up state, perform loopback tests on the nodes along the transmission path to locate the failure point or link. Then check whether the alarm is cleared. If not, go to 4.
 - If not, go to step 4.
- Step 4** Check whether the peer port is physically Down and a corresponding alarm is generated, rectify the fault on the peer port.
- If so, repair the peer port. Check whether the alarm is cleared. If not, go to step 5.
 - If not, go to step 5.
- Step 5** Test whether the fiber is working normally.
- If so, replace the fiber and check whether the alarm is cleared. If not, go to step 6.
 - If not, go to step 6.
- Step 6** Replace the optical module of the local port and check whether the alarm is cleared.
- If so, the alarm handling ends.
 - If not, go to step 7.
- Step 7** Collect alarms, logs, and configurations, and contact technical support personnel.
- End

Related Information

None

3.3.43 ALM-3276800023 Network heartbeat

Description

SRM/3/NETWORKHEARTBEATTRAP: OID [OID] Network heart beat.

The device periodically sends heartbeat packets to the NMS. The NMS considers the device present if it receives heartbeat packets from the device.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800023	Minor	Communication alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.

Impact on the System

None

Possible Causes

The device reports this alarm after it is enabled to send heartbeat packets to the NMS.

Procedure

This message is informational only, and no action is required.

Related Information

None

3.3.44 ALM-3276800024 PoE chip fault 68084

Description

SRM/3/POECHIPFAULT: OID [OID] PoE chip fault. (EntityPhysicalIndex=[INTEGER], BaseTrapSeverity=[INTEGER], BaseTrapProbableCause=[INTEGER], BaseTrapEventType=[INTEGER], EntPhysicalContainedIn=[INTEGER], EntPhysicalName=[OCTET], RelativeResource=[OCTET], ReasonDescription=[OCTET])

The PoE chip is faulty.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800024	Minor	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.

Name	Meaning
EntityPhysicalIndex	Indicates a physical entity index.
BaseTrapSeverity	Indicates the alarm severity.
BaseTrapProbableCause	Indicates the error code of the alarm.
BaseTrapEventType	Indicates the event type.
EntPhysicalContainedIn	Indicates contained physical entity code.
EntPhysicalName	Indicates the physical entity name.
RelativeResource	Indicates a sub-entity.
ReasonDescription	Describes reason of the fault.

Impact on the System

The PoE function is abnormal.

Possible Causes

A hardware fault has occurred.

Procedure

Contact technical support personnel.

Related Information

None

3.3.45 ALM-3276800025 Indicates that the service configurations exceed the recommended threshold

Description

SCMTRAP/4/SRVRESEXCEED: OID [OID] The service configurations on the device exceed the recommended threshold, which may result in CPU overload. Delete redundant services. (Service ID=[INTEGER], Service Description="[OCTET]", Recommended Threshold=[ULONG])

The service configuration on the device has exceeded the recommended threshold, and the CPU may be overloaded. It is recommended that you delete unnecessary configuration.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800025	Warning	Quality of service alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
Service ID	Indicates the ID of the service.
Service Description	Indicates description of the service.
Recommended Threshold	Indicates the recommended configuration threshold for the service. The threshold cannot be changed.

Impact on the System

The system CPU may be overloaded, affecting running of services on the device.

Possible Causes

- Cause 1: The number of IGMP snooping queriers configured on the device exceeds the recommended threshold (Service Description="IGMP snooping querier").
- Cause 2: The number of user VLANs bound to a multicast VLAN exceeds the recommended threshold (Service Description="multicast user VLAN").
- Cause 3: The number of user VLANs bound to a multicast VLAN on an interface exceeds the recommended threshold (Service Description="interface-based multicast user VLAN").
- Cause 4: The number of interfaces configured with storm control exceeds the recommended threshold (Service Description="storm control interface").
- Cause 5: The number of interfaces configured with sFlow exceeds the recommended threshold (Service Description="sFlow sampling interface").
- Cause 6: The number of interfaces configured with GVRP exceeds the recommended threshold (Service Description="GVRP interface").
- Cause 7: The total limit on the number of MAC addresses configured for port security on interfaces exceeds the recommended threshold (Service Description="port security MAC address").
- Cause 8: The number of interfaces configured with DLDP exceeds the recommended threshold (Service Description="DLDP interface").

Procedure

- Cause 1: The number of IGMP snooping queriers configured on the device exceeds the recommended threshold.
When this situation occurs for the first time, the device generates an alarm message to notify you that the configuration exceeds the recommended threshold. Determine whether to modify the current configuration according to actual service requirements.
- Cause 2: The number of user VLANs bound to a multicast VLAN exceeds the recommended threshold.
When this situation occurs for the first time, the device generates an alarm message to notify you that the configuration exceeds the recommended threshold. Determine whether to modify the current configuration according to actual service requirements.
- Cause 3: The number of user VLANs bound to a multicast VLAN on an interface exceeds the recommended threshold.
When this situation occurs for the first time, the device generates an alarm message to notify you that the configuration exceeds the recommended threshold. Determine whether to modify the current configuration according to actual service requirements.
- Cause 4: The number of interfaces configured with storm control exceeds the recommended threshold.
When this situation occurs, the device generates an alarm message to notify you that the configuration exceeds the recommended threshold. Determine whether to modify the current configuration according to actual service requirements.
- Cause 5: The number of interfaces configured with sFlow exceeds the recommended threshold.
When this situation occurs, the device generates an alarm message to notify you that the configuration exceeds the recommended threshold. Determine whether to modify the current configuration according to actual service requirements.
- Cause 6: The number of interfaces configured with GVRP exceeds the recommended threshold.
When this situation occurs, the device generates an alarm message to notify you that the configuration exceeds the recommended threshold. Determine whether to modify the current configuration according to actual service requirements.
- Cause 7: The total limit on the number of MAC addresses configured for port security on interfaces exceeds the recommended threshold.
When this situation occurs, the device generates an alarm message to notify you that the configuration exceeds the recommended threshold. Determine whether to modify the current configuration according to actual service requirements.
- Cause 8: The number of interfaces configured with DLDP exceeds the recommended threshold.
When this situation occurs, the device generates an alarm message to notify you that the configuration exceeds the recommended threshold. Determine whether to modify the current configuration according to actual service requirements.

Related Information

None

3.3.46 ALM-3276800026 Indicates that the service configurations failed

Description

SCMTRAP/3/SRVSERCONFIGFAILED: OID [oid] The service configurations on the device failed because of no enough resources or hash conflict, please undo it. (Service ID=[INTEGER], Service Description="[OCTET]", Service Fail Description="[OCTET]")

The service configurations failed because resources were insufficient or a hash conflict occurred.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800026	Minor	Quality of service alarm

Parameters

Name	Meaning
oid	Indicates the MIB object ID of the alarm.
Service ID	Indicates the service ID.
Service Description	Indicates service description.
Service Fail Description	Indicates service failure description.

Impact on the System

The configurations do not take effect and services are unavailable.

Possible Causes

Resources were insufficient or a hash conflict occurred when services were being configured.

Procedure

Obtain information about the service configurations that fail to be delivered according to **Service Fail Description** and delete the corresponding service configuration commands.

- If the service configurations are required, collect alarm information and configuration information, and then contact technical support personnel.
- If the service configurations are not required, the alarm handling ends.

Related Information

None

3.3.47 ALM-3276800028 Indicates that board fail

Description

ENTITYTRAP/2/BOARDFAIL: OID [OID] Board fails. (Index=[INTEGER], EntityPhysicalIndex=[INTEGER], PhysicalName="[OCTET]", EntityTrapEntType=[INTEGER], EntityTrapFaultID=[INTEGER], EntityTrapReasonDescr="[OCTET]")

Some functions did not take effect.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800028	Major	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
Index	Indicates the index of the alarm.
EntityPhysicalIndex	Indicates the index of a physical entity.
PhysicalName	Indicates the name of a physical entity.
EntityTrapEntType	Indicates the entity type.
EntityTrapFaultID	Indicates the error code.
EntityTrapReasonDescr	Indicates the description of the alarm cause.

Impact on the System

See the description in the procedure.

Possible Causes

See the description in the procedure.

Procedure

Rectify the fault based on the error code.

Error Code	Possible Causes and Impact on the System	Procedure
1320 96	The power module that provides power for the switch was faulty.	Collect alarm information and configuration information, and then contact technical support personnel.
1321 05	The sensor was faulty.	Restart the faulty devicecard and check whether the corresponding clear alarm is displayed. If not, replace the faulty devicecard.
1321 06	The flash memory on the card has failed.	Collect alarm information and configuration information, and then contact technical support personnel.
1321 07	The PHY chip is faulty.	Use other ports that can work normally or replace the card.
1321 21	The USB controller was faulty.	• If there is no storage device on the USB interface, services will not be affected. This alarm is informational only, and no action is required. • If you need to use the USB interface, choose the other USB interfaces on this board or the USB interfaces on other boards.
1321 24	The I2C bus was faulty.	Restart the faulty board and then check whether the corresponding clear alarm is displayed. If not, replace the faulty board in the slot.
1321 27	The clock module on the board was faulty.	Restart the faulty board and then check whether the corresponding clear alarm is displayed. If not, replace the faulty board in the slot.
1321 28	The Phase-Locked Loop (PLL) was faulty.	Restart the faulty board and then check whether the corresponding clear alarm is displayed. If not, replace the faulty board in the slot.

Error Code	Possible Causes and Impact on the System	Procedure
1321 31	The Digital Signal Processor (DSP) was faulty.	Restart the faulty board and then check whether the corresponding clear alarm is displayed. If not, replace the faulty board in the slot.
1321 37	Chips (including CPLD, RTC, EEPROM, and temperature control chip) were faulty.	Restart the faulty board and then check whether the corresponding clear alarm is displayed. If not, replace the faulty board in the slot.
1321 46	The PoE power supply was faulty.	1. Replace the faulty PoE power supply and then check whether the corresponding clear alarm is displayed. If not, go to 2. 2. Replace the faulty PoE DIMM and then check whether the corresponding clear alarm is displayed. If not, go to 3. 3. Collect alarm information and configuration information, and then contact technical support personnel.
1321 47	The indicator was faulty.	Collect alarm information and configuration information, and then contact technical support personnel.
1321 71	The ambient temperature exceeds 45°C.	Open an air-conditioner and enhance heat dissipation to reduce the ambient temperature within 45°C.
1321 76	The PHY chip remains at a low temperature.	Check whether the alarm with the error code 132128 is displayed. • If not, that is, no PLI failure occurs, no action is required. • If so, the PLI is out of lock because the PHY chip remains at a low temperature, and the device will restart. No action is required.
1321 85	The internal IIC module of the card was faulty.	Wait for a period to check whether the fault is rectified. If not, replace the faulty component or the card.
1321 99	A fault occurred on the UART serial port on the internal channel of the MCU component on the PoE device.	Wait for a period to check whether the fault is rectified. If not, replace the faulty component or the card.

Error Code	Possible Causes and Impact on the System	Procedure
1322 00	The device silicon crystal was affected by the external environment, resulting in an uncorrectable error. An error that cannot be rectified by ECC (that is, multiple bit ECC errors) occurred on the storage units (memory and flash memory) of the device. If an instruction error or a file system error occurred, the device cannot operate properly.	Wait for a period to check whether the fault is rectified. If not, replace the faulty component or the card.
1322 01	A CPU DDR fault occurred and the DDR multi-bit error occurred 60 times on the device within one hour. When the DDR multi-bit error occurred 100 times on the device within one hour, the device is restarted and the restart reason is recorded.	Wait for a period to check whether the fault is rectified. If not, replace the faulty component or the card.
1322 08	The PCI of this card failed.	Restart the faulty devicecard and check whether the corresponding clear alarm is displayed. If not, replace the faulty devicecard.
1322 12	An internal error occurred in the CPU cache. The device detected a multi-bit error in the CPU cache and will restart.	After the fault occurs, the device restarts automatically. If this alarm is displayed multiple times, replace the faulty component or device.
1322 15	The 1.5 V CPU sensor was faulty. The voltage of the 1.5 V CPU sensor is not within the normal range.	After the fault occurs, the device restarts automatically. If this alarm is displayed multiple times, replace the faulty component or device.
1322 17	Some uplink optical interfaces become unavailable. - GPON optical modules (MA5671A) and other optical modules are installed on uplink optical interfaces. - Two or more GPON optical modules (MA5671A) are installed on two uplink optical interfaces.	- Determine which uplink optical interface needs to be used based on the networking. - Remove optical modules from the uplink optical interfaces that do not need to be used.

Error Code	Possible Causes and Impact on the System	Procedure
1322 18	The chip of the 0.9 V voltage is abnormal.	Restart the device. If the alarm persists, replace the device in the specified slot.
1322 19	The channel between cards is faulty or some card components are faulty. If some faults are detected on the standby MPU, an active/standby switchover cannot be performed using the slave switchover command.	1. Run the display switchover-prohibit status command to check the fault detection item status of MPUs. 2. Run the display ecm information command to check ECM channel information. 3. Collect alarm information and configuration information, and then contact technical support personnel.
1322 20	The switch detects a TCAM parity error.	Restart the faulty devicecard and check whether the corresponding clear alarm is displayed. If not, replace the faulty devicecard.
1322 23	The read and write operations are frequently performed in the partition, damaging storage components. The bad block rate of the SystemMain (nsysmain) partition exceeded the alarm threshold 2%, so the available storage space is low.	1. Restart the device. Ten seconds later, check whether the alarm persists. If so, go to 2. 2. Run the format flash: command to format the flash. Ten seconds later, check whether the alarm is cleared. If so, go to 3 3. Contact technical support personnel to replace the device or flash component.
1322 24	The read and write operations are frequently performed in the partition, damaging storage components. The bad block rate of the SystemBack (nsysbak) partition exceeded the alarm threshold 2%, so the available storage space is low.	1. Restart the device. Ten seconds later, check whether the alarm persists. If so, go to 2. 2. Run the format flash: command to format the flash. Ten seconds later, check whether the alarm is cleared. If so, go to 3 3. Contact technical support personnel to replace the device or flash component.

Error Code	Possible Causes and Impact on the System	Procedure
1322 25	The read and write operations are frequently performed in the partition, damaging storage components. The bad block rate of the SystemData (nsysdata) partition exceeded the alarm threshold 2%, so the available storage space is low.	1. Restart the device. Ten seconds later, check whether the alarm persists. If so, go to 2. 2. Run the format flash: command to format the flash. Ten seconds later, check whether the alarm is cleared. If so, go to 3 3. Contact technical support personnel to replace the device or flash component.
1322 26	The read and write operations are frequently performed in the partition, damaging storage components. The bad block rate of the SystemFile (NVRP or nand root file system) partition exceeded the alarm threshold 2%, so the available storage space is low.	1. Restart the device. Ten seconds later, check whether the alarm persists. If so, go to 2. 2. Run the format flash: command to format the flash. Ten seconds later, check whether the alarm is cleared. If so, go to 3 3. Contact technical support personnel to replace the device or flash component.
1322 27	The read and write operations are frequently performed in the partition, damaging storage components. The bad block rate of the NVRP partition exceeded the threshold 1.5%, so the available storage space is low.	1. Restart the device. Ten seconds later, check whether the alarm persists. If so, go to 2. 2. Run the format flash: command to format the flash. Ten seconds later, check whether the alarm is cleared. If so, go to 3 3. Contact technical support personnel to replace the device or flash component.
1322 28	The power consumed by the connected powered device is too high, the total PoE power and the DC output power of the S5720I-10X-PWH-SI-AC exceeds the total power, the device automatically disables the DC power supply function of the 12 V line 1.	Reduce the power consumed by the powered device.

Error Code	Possible Causes and Impact on the System	Procedure
1322 29	The power consumed by the connected powered device is too high, the total PoE power and the DC output power of the S5720I-10X-PWH-SI-AC exceeds the total power, the device automatically disables the DC power supply function of the 12 V line 2.	Reduce the power consumed by the powered device.
1322 30	The power consumed by the connected powered device is too high, the total PoE power and the DC output power of the S5720I-10X-PWH-SI-AC exceeds the total power, the device automatically disables the DC power supply function of the 24 V line.	Reduce the power consumed by the powered device.
1322 31	The power consumed by the connected powered device is too high, the 12 V DC output power of the S5720I-10X-PWH-SI-AC exceeds the alarm threshold 104 W for the 12 V DC output power, the device automatically disables the DC power supply function of 12 V lines.	Reduce the power consumed by the powered device.
1322 32	The power consumed by the connected powered device is too high, the 24 V DC output power of the S5720I-10X-PWH-SI-AC exceeds the alarm threshold 78 W for the 24 V DC output power, the device automatically disables the DC power supply function of the 24 V line.	Reduce the power consumed by the powered device.
1322 33	A CPU internal module failed.	Restart the faulty devicecard and check whether the corresponding clear alarm is displayed. If not, replace the faulty devicecard.

Error Code	Possible Causes and Impact on the System	Procedure
1322 34	The chip was faulty, so the MPU management channel fails.	Restart the device and check whether the alarm persists. If so, collect alarm information and configuration information, and then contact technical support personnel.
1326 25	The chip does not work normally.	Restart the faulty board and then check whether the corresponding clear alarm is displayed. If not, replace the faulty board in the slot.
1351 90	The lead-acid battery cannot power the switch, and the switch will be powered off because of insufficient power.	Connect an AC power module to the switch or replace this lead-acid battery.
1322 36	An MCU serial port is faulty.	Wait for a period to check whether the fault is rectified. If not, replace the faulty component or the card.
1322 37	An MCU I2C fault occurs.	Wait for a period to check whether the fault is rectified. If not, replace the faulty component or the card.
1322 39	The NOR flash memory is erased frequently. That is, the NOR flash memory is erased 100 times within 24 hours.	Collect alarm information and configuration information, and then contact technical support personnel.
1322 40	The disk usage exceeded the threshold. This may be because there are many log files on the switch or unnecessary .cc files were not deleted on the switch.	Three methods are available to solve this problem: • Run the reset logbuffer command in the user view to delete unnecessary log information from the log buffer. • Run the delete /unreserved command in the user view to delete the specified .cc file from the memory. • Run the reset recycle-bin command in the user view to delete the files in the specified directory from the recycle bin.
1322 49	The NOR flash memory has reached 90% of its life cycle.	Collect alarm information and configuration information, and then contact technical support personnel.
1322 49	The NOR flash memory has reached 90% of its life cycle.	Collect alarm information and configuration information, and then contact technical support personnel.

Error Code	Possible Causes and Impact on the System	Procedure
1322 52	The chassis type obtained on the card is incorrect.	Collect alarm information and configuration information, and then contact technical support personnel.
1322 53	The number of MAC addresses on the CSS master MPU is different from the number of CSS MAC addresses.	1. Run the display css system-mac command to check the number of CSS MAC addresses and the number of MAC addresses on each MPU. 2. Change the number of CSS MAC addresses and the number of MAC addresses on each MPU to the minimum values based on the minimum number of CSS MAC addresses.
1322 81	Card burnt due to high PoE power.	Collect alarm information and configuration information, and then contact technical support personnel.
1322 82	The specified interface receives preamble error packets.	Run the port serdes-mode command to configure the working Serdes mode of the MultiGE interface.
1322 83	The specified interface cannot go up due to insufficient frequency.	1. Check whether the device connected to the interface specified in the alarm can be connected to another interface on the switch. • If so, go to step 2. • If not, go to step 3. 2. Connect the device to another interface on the switch, and check whether the alarm persists. • If so, repeat step 2. • If not, no further action is required. 3. Run the port serdes-mode command again to configure the Serdes mode in which the MultiGE interface works. Ensure that the Serdes mode in which the MultiGE interface specified in the alarm should work is specified in the command.
1323 15	The negotiated transmission rate of the SATA hard disk does not meet the requirement.	Collect alarm information and configuration information, and then contact technical support personnel.

Error Code	Possible Causes and Impact on the System	Procedure
1323 16	The remaining service life of the SATA hard disk is insufficient.	Collect alarm information and configuration information, and then contact technical support personnel.
1323 17	The SATA hard disk is abnormal.	Collect alarm information and configuration information, and then contact technical support personnel.
1323 18	The SATA hard disk is read-only.	Collect alarm information and configuration information, and then contact technical support personnel.

Related Information

None

3.3.48 ALM-3276800029 Indicates that board invalid

Description

ENTITYTRAP/1/BOARDINVALID: OID [OID] Board is invalid for some reason.
(Index=[INTEGER], EntityPhysicalIndex=[INTEGER], PhysicalName="[OCTET]", EntityTrapEntType=[INTEGER], EntityTrapFaultID=[INTEGER])

A card experienced a complete failure.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800029	Critical	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
Index	Indicates the index.
EntityPhysicalIndex	Indicates the physical index.
PhysicalName	Indicates the entity name, such as SFU, LPU, and MPU. The entity name varies with the type of the board.

Name	Meaning
EntityTrapEntType	Indicates the entity type.
EntityTrapFaultID	Indicates the error code.

Impact on the System

See the description in the procedure.

Possible Causes

See the description in the procedure.

Procedure

Rectify the fault based on the error code.

Error Code	Possible Causes	Procedure
1326 10	The CMU does not match the device model, so the CMU does not work and the power supply units and fans may run abnormally.	1. Run the display device command to check device model information. 2. Use a CMU that matches the device model. For the mappings between CMUs and device models, see the Hardware Query Tool .
1326 13	The serial gigabit media independent interface (SGMII) channel between the CPU and field programmable gate array (FPGA) on the card has failed. Packets cannot be sent to the CPU for processing.	Restart the faulty card and check whether the alarm persists. If the alarm is not cleared, replace the faulty card in the slot.
1326 25	The chip on the board has failed. If an LPU fails, all services running on the LPU may be interrupted. If the standby MPU fails, the system reliability will be affected. If the active MPU fails, an active/standby switchover will occur.	Restart the faulty board and then check whether the corresponding clear alarm is displayed. If not, replace the faulty board in the slot.

Error Code	Possible Causes	Procedure
1326 26	The power cable connected to the device is loose, the external power line is faulty or the power module of the device has failed.	1. Check whether the power cable is loose. • If so, reconnect the power cable securely and power on the device. • If not, go to step 2. 2. Check whether the external power line is faulty. • If so, repair or replace the faulty line and power on the device again. • If not, go to step 3. 3. Check whether the power module of the device is faulty. • If so, replace the power module. If the device uses a built-in power module, replace the device. • If not, Collect alarm information and configuration information, and then contact technical support personnel..
1326 27	The board failed to be registered.	Restart the faulty board and then check whether the corresponding clear alarm is displayed. If not, replace the faulty board in the slot.
	Run the power off slot <i>slot-id</i> command to power off the faulty card.	Check whether the operation is required by services. • If so, this alarm is informational and no action is required. • If not and the card is still required, run the power on slot <i>slot-id</i> command to power on the card.
	Run the reset slot <i>slot-id</i> command to reset the card.	This alarm is informational and no action is required.
1326 32	The Peripheral Component Interconnect (PCI) bus has failed.	Restart the faulty board and then check whether the corresponding clear alarm is displayed. If not, replace the faulty board in the slot.

Error Code	Possible Causes	Procedure
132648	If you hold down the OFL button on the board for 6s, the board stops working and generates this alarm. Services are not affected.	When the OFL indicator on the board turns red, remove the board. If the board is not removed in 10 minutes, it resets and starts to run.

3.3.49 ALM-3276800030 The number of VAP instances has exceeded the maximum

Description

WLAN/2/VAP_NUM_EXCEEDED: OID [OID] The number of VAP instances has exceeded the maximum. (Vap = [INTEGER])

The number of VAP instances exceeds the maximum specifications of the system.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800030	Major	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object of the alarm.
Vap	Indicates the maximum number of VAPs.

Impact on the System

VAPs that exceed the specifications cannot be created.

Possible Causes

The number of VAP instances reaches the maximum specifications of the system.

Procedure

Step 1 Run the **display vap all** command to view all VAPs on the device.

- Step 2** Run the **display ap by-ssid** *ssid* command to view information about an AP group with a specified SSID.
- Step 3** Run the **ap-group name** *group-name* command to enter the AP group view.
- Step 4** Run the **undo vap-profile** *profile-name* **wlan** *wlan-id* { **radio** { *radio-id* | **all** } } command to delete one or more VAPs that are not needed.
- If the alarm persists, go to Step 5.
 - If the alarm is cleared, go to Step 6.
- Step 5** Collect alarm messages, log messages, and configurations, and then contact the technical support personnel.
- Step 6** End.
- End

Related Information

None

3.3.50 ALM-3276800031 Indicates that card fail

Description

ENTITYTRAP/2/CARDFAIL: OID [OID] Card fails. (Index=[INTEGER], EntityPhysicalIndex=[INTEGER], PhysicalName="[OCTET]", EntityTrapEntType=[INTEGER], EntityTrapFaultID=[INTEGER])

Some functions on a card fail.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800031	Major	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
Index	Indicates the alarm index.
EntityPhysicalIndex	Indicates the physical entity index.
PhysicalName	Indicates the name of the physical entity where the alarm is generated.
EntityTrapEntType	Indicates the alarm type.

Name	Meaning
EntityTrapFaultID	Indicates the error code of the alarm, which is 135194.

Impact on the System

The IIC bus cannot be accessed normally.

Possible Causes

The IIC bus has failed.

Procedure

- Remove and install the card and then check whether the alarm is cleared.
 - If so, the alarm handling ends.
 - If not, go to step 2.
- Replace the card and check whether the alarm is cleared.
 - If so, the alarm handling ends.
 - If not, collect alarm information and configuration information, and then contact technical support personnel.

Related Information

None

3.3.51 ALM-3276800032 Indicates that card invalid

Description

ENTITYTRAP/1/CARDINVALID: OID [OID] Card is invalid for some reason.
(Index=[INTEGER], EntityPhysicalIndex=[INTEGER], PhysicalName="[OCTET]",
EntityTrapEntType=[INTEGER], EntityTrapFaultID=[INTEGER],
EntityTrapReasonDescr="[OCTET]")

The subcard does not work.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800032	Critical	environmentalAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
Index	Indicates the alarm ID.
EntityPhysicalIndex	Indicates the index.
PhysicalName	Indicates the physical entity name.
EntityTrapEntType	Indicates the alarm type.
EntityTrapFaultID	Indicates the error code.
EntityTrapReasonDescr	Indicates the description of the alarm cause.

Impact on the System

See the description in the procedure.

Possible Causes

See the description in the procedure.

Procedure

Rectify the fault based on the error code.

Error Code	Possible Causes	Procedure
1354 35	The subcard does not match the slot where the subcard was installed. • The subcard was installed in an unsupported slot. • An unsupported subcard was installed in the slot.	Install a subcard matching the slot. For the subcards supported in different subcard slots, see Hardware Description > Chassis > Appearance and Structure.

Error Code	Possible Causes	Procedure
1354 75	The subcard is not installed securely or the subcard is faulty and cannot be registered.	1. Remove the subcard to check whether it has bent pins. • If so, repair or replace the subcard. • If not, go to step 2. 2. Reinstall the subcard securely at a time. If it is not installed securely at a time, remove it and then install it securely again. 3. Check whether the device receives an alarm indicating that the fault has been rectified. • If so, the alarm handling ends. • If not, collect alarm information and configuration information, and then contact technical support personnel.
1436 20	The power module that provides power for the subcard PHY chip was working abnormally.	1. Remove and install the subcard to check whether the resume alarm is displayed. • If so, the alarm handling ends. • If not, go to step 2. 2. Replace this faulty subcard.
1436 21	The subcard failed to be powered on because it was not properly installed or a hardware fault occurred.	1. Remove and install the subcard to check whether the resume alarm is displayed. • If so, the alarm handling ends. • If not, go to step 2. 2. Replace this faulty subcard.
1436 22	The subcard PHY chip or LSW became faulty.	1. Remove and install the subcard to check whether the resume alarm is displayed. • If so, the alarm handling ends. • If not, go to step 2. 2. Replace this faulty subcard.

3.3.52 ALM-3276800033 Optical Module Detection Failed

Description

ENTITYTRAP/3/OPTICALFAIL: OID [OID] Optical Module fails. (Index=[INTEGER], EntityPhysicalIndex=[INTEGER], PhysicalName="[OCTET]", EntityTrapFaultID=[INTEGER], EntityTrapReasonDescr="[OCTET]")

Optical module detection failed.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800033	Minor	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
Index	Indicates an index.
EntityPhysicalIndex	Indicates a physical index.
PhysicalName	Indicates the entity name.
EntityTrapFaultID	Indicates the error code.
EntityTrapReasonDescr	Indicates the reason description of the alarm.

Impact on the System

The interface that has the optical module installed may fail to go Up.

Possible Causes

Cause 1:

No cable or optical module was detected.

Cause 2:

The cable type was detected but the specific type cannot be identified. For example, whether the cable is active is passive and the cable length cannot be identified.

Cause 3:

The cable does not comply with interface specifications.

Procedure

- Step 1** Run the **display transceiver interface** *interface-type interface-number* command to check whether **Transceiver Type** matches the interface type. For example, a GE interface needs to use an optical module that provides the GE rate.
- If so, go to step 2.
 - If not, replace the optical module with one that matches the interface type.
- Step 2** Check whether the optical module is a Huawei-certified one. For details, see *How Can I Determine Whether an Optical Module Is Huawei-Certified*.
- If so, collect alarm information and configuration information, and then contact technical support personnel.
 - If not, replace the optical module with a Huawei-certified one.
- End

Related Information

None

3.3.53 ALM-3276800034 The IGMP snooping bandwidth of VAP has reached the maximum

Description

WLAN/4/VAP_IGMP_SNOOPING_BANDWIDTH_EXCEEDED: OID [OID] The IGMP snooping bandwidth of VAP has reached the maximum. (APMAC=[OPAQUE], RADIOID=[INTEGER], WLANID=[INTEGER], APName=[STRING], MaxBandWidth=[INTEGER], APID=[INTEGER])

The multicast bandwidth of a VAP exceeds the threshold.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800034	Warning	Quality of service alarm

Parameters

Name	Meaning
OID	ID of a MIB object.
APMAC	MAC address of an AP.
RADIOID	Radio ID.
WLANID	WLAN ID.
APName	AP name.

Name	Meaning
MaxBandWidth	Maximum multicast bandwidth of a VAP.
APID	AP ID.

Impact on the System

New users cannot join multicast groups.

Possible Causes

The multicast traffic of the VAP exceeds the maximum multicast bandwidth configured for the VAP.

Procedure

- Step 1** Run the **display traffic-profile { all | name *profile-name* }** command to check whether the maximum multicast bandwidth of a VAP is properly configured.
- If so, the actual multicast traffic is too large, and it is normal that users are prevented from joining multicast groups, and no action is required. Go to Step 5.
 - If not, go to Step 2.
- Step 2** Run the **igmp-snooping max-bandwidth *max-bandwidth*** command to configure a large value for the maximum multicast bandwidth of a VAP.
- Step 3** Check whether the alarm persists.
- If so, go to Step 4.
 - If not, go to Step 5.
- Step 4** Collect trap, log, and configuration information, and contact technical support personnel.
- Step 5** End.
- End

Related Information

None

3.3.54 ALM-3276800035 The IGMP Snooping User of VAP Has Reached the Upper Threshold

Description

WLAN/4/VAP_IGMP_SNOOPING_USER_EXCEEDED: OID [OID] The IGMP snooping user of VAP has reached the maximum. (APMAC=[OPAQUE], RADIOID=[INTEGER],

WLANID=[INTEGER], APName=[STRING], MaxUserNum=[INTEGER],
APID=[INTEGER])

The number of multicast bandwidth memberships on a VAP exceeds the threshold.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800035	Warning	Quality of service alarm

Parameters

Name	Meaning
OID	ID of a MIB object.
APMAC	MAC address of an AP.
RADIOID	Radio ID.
WLANID	WLAN ID.
APName	AP name.
MaxUserNum	Maximum number of multicast group memberships on a VAP.
APID	AP ID.

Impact on the System

New users cannot join multicast groups.

Possible Causes

The number of multicast users on the VAP exceeds the maximum number of multicast group memberships configured for the VAP.

Procedure

- Step 1** Run the **display traffic-profile { all | name *profile-name* }** command to check whether the maximum number of multicast group memberships on the VAP is properly configured.
- If so, the actual multicast traffic is too large, and it is normal that users are prevented from joining multicast groups. No action is required and proceed to Step 5.
 - If not, go to Step 2.
- Step 2** Run the **igmp-snooping max-user *max-user*** command to set a large value for the maximum number of multicast group memberships on the VAP.

Step 3 Check whether the alarm persists.

- If so, go to Step 4.
- If not, go to Step 5.

Step 4 Collect trap, log, and configuration information, and contact technical support personnel.

Step 5 End.

----End

Related Information

None

3.3.55 ALM-3276800036 An AP Detects that the Soft-GRE Tunnel Is Down

Description

WLAN/4/AP_DETECT_SOFTGRE_DOWN:OID [OID] AP detect softgre tunnel down notify.(APMAC=[OPAQUE], DstIP=[IPADDR], APName=[STRING], APID=[INTEGER])

An AP detects that the soft-GRE tunnel is Down.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800036	Major	Quality of service alarm

Parameters

Name	Meaning
OID	Indicates the ID of the alarm MIB object.
APMAC	Indicates the MAC address of an AP.
DstIP	Indicates the destination IP address.
APName	Indicates the AP name.
APID	Indicates the AP ID.

Impact on the System

User traffic cannot be forwarded through the Soft-GRE tunnel.

Possible Causes

AP detect soft-GRE tunnel down notify.

Procedure

- Step 1** Check whether the Soft-GRE function is enabled on the VE interface of the Soft-GRE tunnel.
- Step 2** Check whether the IP address is correctly configured on the loopback interface.
- Step 3** Check whether the Soft-GRE group is bound to the VE interface and loopback interface.
- Step 4** Check whether the ME60 can ping the AP.
- Step 5** Collect trap, log, and configuration information, and contact technical support personnel.

----End

3.3.56 ALM-3276800037 Communicate Error

Description

ENTITYTRAP/4/ENTITYCOMMERROR: OID [OID] Communication error has been detected. (Index=[INTEGER], EntityPhysicalIndex=[INTEGER], PhysicalName="[OCTET]", EntityTrapEntType=[INTEGER], EntityTrapFaultID=[INTEGER], EntityCommunicateType=[INTEGER])

A communication channel failed.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800037	Warning	Communication alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
Index	Indicates the alarm index.
EntityPhysicalIndex	Indicates the index of a physical entity.
PhysicalName	Indicates the name of the physical entity.
EntityTrapEntType	Indicates the alarm type for the physical entity.

Name	Meaning
EntityTrapFaultID	Indicates the error code of the alarm.
EntityCommunicateType	Indicates the type of the communication failure.

Impact on the System

See the description in the procedure.

Possible Causes

See the description in the procedure.

Procedure

Rectify the fault based on the error code.

Error Code	Possible Causes and Impact on the System	Procedure
140289	Protocol packets cannot be forwarded over the communication channel. The possible causes are: • The HG rate on either end of the communication channel is set incorrectly. • The SFU or LPU is not properly installed or it has some pins on the connector bent.	Collect alarm information and configuration information, and then contact technical support personnel.
140312	Some services or all services on the device are interrupted because the CANbus is unavailable. The possible causes are: • The card is not installed properly. • The CANbus does not work normally, causing communication interruption.	1. Remove and reinstall the card to check whether a clear alarm is generated. • If so, the alarm handling ends. • If not, collect alarm information and configuration information, and then contact technical support personnel.
140319	Services are interrupted because the link between an SFU and LPU is Down within five consecutive seconds.	Collect alarm information and configuration information, and then contact technical support personnel.

Error Code	Possible Causes and Impact on the System	Procedure
1403 20	The same channel between an MPU and two or more LPUs is abnormal. Packets cannot be forwarded or are lost between the MPU and LPUs. The possible causes are: • The CPU is busy for a short period, causing a failure to forward channel detection packets. • The MPU becomes faulty.	1. Check whether the device has reported a clear alarm. • If so, the alarm handling ends. • If not, go to step 2. 2. Check the EntityCommunicate-Type value in the alarm. • If the value is 5, replace the corresponding MPU in the slot specified by PhysicalName in the alarm. • If the value is 6, replace another MPU in the slot specified by PhysicalName in the alarm.

Related Information

None

3.3.57 ALM-3276800038 The Voltage of the Power Supply Is Higher than the Upper Threshold or Falls Below the Lower Threshold

Description

ENTITYTRAP/1/ENTITYVOLTALARM: OID [OID] Voltage of power rises over or falls below the alarm threshold. (EntityPhysicalIndex=[INTEGER], EntityThresholdType=[INTEGER], EntityThresholdValue=[INTEGER], EntityThresholdCurrent=[INTEGER], EntityTrapFaultID=[INTEGER])

The voltage of the power supply is higher than the upper threshold or falls below the lower threshold.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800038	Critical	environmentalAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
EntityPhysicalIndex	Indicates the index of the physical entity.
EntityThresholdType	Indicates the threshold type of the physical entity.
EntityThresholdValue	Indicates the threshold value of the physical entity.
EntityThresholdCurrent	Indicates the current value.
EntityTrapFaultID	Indicates the error code.

Impact on the System

The board may be powered off, causing interruption of services on the board.

Possible Causes

See the description in the procedure.

Procedure

Rectify the fault based on the error code.

Error Code	Possible Causes	Procedure
141056	A power module has failed or the board has failed, So the voltage of the power supply is higher than the upper threshold.	1. Check whether any power module has a hardware failure: Use a power module that can work normally to replace the power modules in the switch one by one. Each time a power module is replaced, run the display voltage slot slot-id command to check the voltage on each board. If all boards have normal voltage, the replaced power module has a hardware failure. • If so, go to step 2. • If not, go to step 3. 2. Replace the faulty power module. Run the display voltage slot slot-id command to check whether the voltage of the board that has generated the alarm is normal. • If so, the alarm handling ends. • If not, go to step 3. 3. Reset the board and check whether the alarm is cleared. • If so, the alarm handling ends. • If not, go to step 4. 4. Replace the board and check whether the alarm is cleared. • If so, the alarm handling ends. • If not, collect alarm information and configuration information, and then contact technical support personnel.

Error Code	Possible Causes	Procedure
141057	A power module has failed, the board has failed or the power provided to the switch is insufficient because there are not enough power modules in the switch. So the voltage of the power supply falls below the lower threshold.	1. Check whether all power modules in the chassis are supported by the chassis and whether the power modules are sufficient to supply power to all boards in the chassis. For the models of power modules supported by each chassis model, see Hardware Description > Chassis > Slots > Power Slot Configuration. • If so, go to step 3. • If not, go to step 2. 2. Replace the unsupported power modules with those supported by the chassis, and add power modules based on the required power to ensure power sufficiency. Check whether the alarm is cleared. • If so, the alarm handling ends. • If not, go to step 3. 3. Check whether any power module has a hardware failure: Use a power module that can work normally to replace the power modules in the switch one by one. Each time a power module is replaced, run the display voltage slot slot-id command to check the voltage on each board. If all boards have normal voltage, the replaced power module has a hardware failure. • If so, go to step 4. • If not, go to step 5. 4. Replace the faulty power module. Run the display voltage slot slot-id command to check whether the voltage of the board that has generated the alarm is normal. • If so, the alarm handling ends. • If not, go to step 5. 5. Reset the board and check whether the alarm is cleared. • If so, the alarm handling ends. • If not, go to step 6. 6. Replace the board and check whether the alarm is cleared.

Error Code	Possible Causes	Procedure
		• If so, the alarm handling ends. • If not, collect alarm information and configuration information, and then contact technical support personnel.

Related Information

None

3.3.58 ALM-3276800039 VAP create fail

Description

WLAN/4/VAP_CREATE_FAIL: OID [OID] VAP create fail.(Reason=[STRING])
A VAP fails to be created.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800039	Warning	Equipment alarm

Parameters

Name	Meaning
Reason	Indicates the reason for the failure to create a VAP.

Impact on the System

The VAP cannot be created.

Possible Causes

For detailed reasons, see Table 2.

Procedure

- Step 1** Handling the alarm based on different reasons. For detailed handling suggestions, see Table 2.
- End

Related Information

None

3.3.59 ALM-3276800040 AP has the max number of stations notify

Description

WLAN/4/AP_REACH_MAX_USERS:OID [OID] AP has the max number of stations notify.(APMAC=[OPAQUE], APName=[STRING], FailCause=[INTEGER], PermitNum=[INTEGER], APID=[INTEGER])

The maximum number of STAs associated with the AP was reached.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800040	Warning	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
APMAC	Indicates the MAC address of an AP.
APName	Indicates the AP name.
FailCause	Indicates the cause for the STA authentication failure.
PermitNum	Indicates the maximum number of STAs that can be associated with the AP.
APID	Indicates the AP ID.

Impact on the System

The newly added STAs cannot go online.

Possible Causes

The number of STAs connected to an AP has reached the upper limit. New STAs cannot connect to the VAP.

Procedure

Re-plan the network and increase the network capacity.

Related Information

None

3.3.60 ALM-3276800041 RADIO reach the max number of stations notify

Description

WLAN/4/RADIO_REACH_MAX_USER_PHY_SPECS:OID [OID] RADIO reach the max number of stations notify.(APMAC=[OPAQUE], RADIOID=[INTEGER], APID=[INTEGER], APName=[STRING], StaNum=[INTEGER], MaxStaNum=[INTEGER])

The number of access STAs reached the maximum physical specifications supported by a radio.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800041	Warning	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object of the alarm.
APMAC	Indicates the MAC address of an AP.
RADIOID	Indicates the radio ID.
APID	Indicates the AP ID.
APName	Indicates the AP name.
StaNum	Indicates the number of access STAs.
MaxStaNum	Indicates the maximum number of access STAs supported by the radio.

Impact on the System

New STAs cannot go online.

Possible Causes

The number of access STAs reached the maximum physical specifications supported by a radio.

Procedure

Step 1 Replace the AP with a model supporting more access STAs or expand the AP capacity.

- If the alarm persists, go to step 2.
- If the alarm is cleared, go to step 3.

Step 2 Collect alarm and configuration information, and contact technical support personnel.

Step 3 End.

----End

Related Information

None

3.3.61 ALM-3276800042 Indicates that the optical power exceeds the upper warning threshold or falls below the lower warning threshold

3.3.61.1 ALM-3276800042 Indicates that the optical power exceeds the upper warning threshold or falls below the lower warning threshold 136220

Description

ENTITYTRAP/3/OPTMAYINVALID: OID [OID] The optical power exceeds the upper warning threshold or falls below the lower warning threshold. (Index=[INTEGER], EntityPhysicalIndex=[INTEGER], PhysicalName="[OCTET]", EntityTrapFaultID=[INTEGER], EntityTrapReasonDescr="[OCTET]")

The transmit power of an optical module is too high.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800042	Minor	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
Index	Indicates the index.
EntityPhysicalIndex	Indicates the index of the physical entity.
PhysicalName	Indicates the name of the physical entity.
EntityTrapFaultID	Indicates the error code.
EntityTrapReasonDescr	Indicates the description of the alarm cause.

Impact on the System

This alarm does not affect system operating if the interface on which the optical module is installed works properly.

Possible Causes

The transmit power of the optical module is too high.

Procedure

- Step 1** Run the **display transceiver slot *slot-id* verbose** command in the system view to check whether the transmit power **Tx Power** of the optical module is within the allowed range.
- If so, services are not affected. Collect alarms, logs, and configurations and contact technical support personnel.
 - If not, go to step 2.
- Step 2** Check whether the transmit power upper threshold of the optical module is within the acceptable range.
- If so, run the **transceiver diagnosis threshold tx-power** command to change the transmit power upper threshold of the optical module. The alarm handling ends.
 - If not, go to step 3.
- Step 3** Use an optical attenuator to reduce the transmit power of the optical module to the acceptable range. Check whether the alarm is cleared.
- If so, the alarm handling ends.
 - If not, go to step 4.
- Step 4** Replace the optical module, and check whether the alarm is cleared.

- If so, the alarm handling ends.
 - If not, collect alarms, logs, and configurations, and contact technical support personnel.
- End

Related Information

None

3.3.61.2 ALM-3276800042 Indicates that the optical power exceeds the upper warning threshold or falls below the lower warning threshold 136221

Description

ENTITYTRAP/3/OPTMAYINVALID: OID [OID] The optical power exceeds the upper warning threshold or falls below the lower warning threshold. (Index=[INTEGER], EntityPhysicalIndex=[INTEGER], PhysicalName="[OCTET]", EntityTrapFaultID=[INTEGER], EntityTrapReasonDescr="[OCTET]")

The transmit power of an optical module is too low.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800042	Minor	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
Index	Indicates the index.
EntityPhysicalIndex	Indicates the index of the physical entity.
PhysicalName	Indicates the name of the physical entity.
EntityTrapFaultID	Indicates the error code.
EntityTrapReasonDescr	Indicates the description of the alarm cause.

Impact on the System

This alarm does not affect system operating if the interface on which the optical module is installed works properly.

Possible Causes

The transmit power of the optical module is too low.

Procedure

- Step 1** Run the **display transceiver slot *slot-id* verbose** command in the system view to check whether the transmit power **Tx Power** of the optical module is within the allowed range.
- If so, services are not affected. Collect alarms, logs, and configurations and contact technical support personnel.
 - If not, go to step 2.
- Step 2** Check whether the transmit power lower threshold of the optical module is within the acceptable range.
- If so, run the **transceiver diagnosis threshold tx-power** command to change the transmit power lower threshold of the optical module. The alarm handling ends.
 - If not, go to step 3.
- Step 3** Replace the optical module, and check whether the alarm is cleared.
- If so, the alarm handling ends.
 - If not, collect alarms, logs, and configurations, and contact technical support personnel.

----End

Related Information

None

3.3.61.3 ALM-3276800042 Indicates that the optical power exceeds the upper warning threshold or falls below the lower warning threshold 136222

Description

ENTITYTRAP/3/OPTMAYINVALID: OID [OID] The optical power exceeds the upper warning threshold or falls below the lower warning threshold. (Index=[INTEGER], EntityPhysicalIndex=[INTEGER], PhysicalName="[OCTET]", EntityTrapFaultID=[INTEGER], EntityTrapReasonDescr="[OCTET]")

The receive power of an optical module is too high.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800042	Minor	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
Index	Indicates the index.
EntityPhysicalIndex	Indicates the index of the physical entity.
PhysicalName	Indicates the name of the physical entity.
EntityTrapFaultID	Indicates the error code.
EntityTrapReasonDescr	Indicates the description of the alarm cause.

Impact on the System

This alarm does not affect system operating if the interface on which the optical module is installed works properly.

Possible Causes

The receive power is too high.

Procedure

- Step 1** Run the **display transceiver slot *slot-id* verbose** command in the system view to check whether the receive power **Rx Power** of the optical module is within the allowed range.
- If so, collect alarms, logs, and configurations, and contact technical support personnel.
 - If not, go to step 2.
- Step 2** Check whether the receive power of the optical module is within a usable range.
- If so, run the **transceiver diagnosis threshold rx-power** command to change the receive power upper threshold of the optical module. The alarm handling ends.
 - If not, go to step 3.

- Step 3** Check whether an alarm is generated for high transmit power on the peer optical module. If so, rectify the peer optical module fault first.
- Step 4** Check whether the peer optical module and the local optical module are of the same type. If not, replace the local optical module with a new one to ensure they are of the same type.
- Step 5** Add -5 dBm (recommended) attenuators to the optical module.
- Step 6** If the problem persists after the preceding steps, collect alarms, logs, and configurations, and contact technical support personnel.

----End

Related Information

None

3.3.61.4 ALM-3276800042 Indicates that the optical power exceeds the upper warning threshold or falls below the lower warning threshold 136223

Description

ENTITYTRAP/3/OPTMAYINVALID: OID [OID] The optical power exceeds the upper warning threshold or falls below the lower warning threshold. (Index=[INTEGER], EntityPhysicalIndex=[INTEGER], PhysicalName="[OCTET]", EntityTrapFaultID=[INTEGER], EntityTrapReasonDescr="[OCTET]")

The receive power of an optical module is too low.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800042	Minor	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
Index	Indicates the index.
EntityPhysicalIndex	Indicates the index of the physical entity.
PhysicalName	Indicates the name of the physical entity.
EntityTrapFaultID	Indicates the error code.

Name	Meaning
EntityTrapReasonDescr	Indicates the description of the alarm cause.

Impact on the System

This alarm does not affect system operating if the interface on which the optical module is installed works properly.

Possible Causes

The receive power of the optical module was too low.

Procedure

- Step 1** Run the **display transceiver slot *slot-id* verbose** command in the system view to check whether the receive power **Rx Power** of the local interface is within the acceptable range.
- If so, collect alarms, logs, and configurations, and contact technical support personnel.
 - If not, go to step 2.
- Step 2** Check whether the receive power of the optical module is within a usable range.
- If so, run the **transceiver diagnosis threshold rx-power** command to change the receive power lower threshold of the optical module. The alarm handling ends.
 - If not, go to step 3.
- Step 3** Check whether the peer port is physically Up and whether there is no alarm indicating that the transmit power is too low.
- If so, perform an external loopback test on the interface. If the interface is in Up state, perform loopback tests on the nodes along the transmission path to locate the failure point or link. Then check whether the alarm is cleared. If not, go to 4.
 - If not, go to step 4.
- Step 4** Check whether the peer port is physically Down and a corresponding alarm is generated, rectify the fault on the peer port.
- If so, repair the pee port. Check whether the alarm is cleared. If not, go to step 5.
 - If not, go to step 5.
- Step 5** Test whether the fiber is working normally.
- If so, replace the fiber and check whether the alarm is cleared. If not, go to step 6.
 - If not, go to step 6.
- Step 6** Replace the optical module of the local port and check whether the alarm is cleared.

- If so, the alarm handling ends.
- If not, go to step 7.

Step 7 Collect alarms, logs, and configurations, and contact technical support personnel.
----End

Related Information

None

3.3.62 ALM-3276800043 Indicates that the optical power exceeds the upper alarm threshold or falls below the lower alarm threshold

3.3.62.1 ALM-3276800043 Indicates that the optical power exceeds the upper alarm threshold or falls below the lower alarm threshold 136193

Description

SRM/3/TXPOWER_EXCEEDMAJOR: OID [OID] Optical module exception, Tx power is too high. (EntityPhysicalIndex=[INTEGER], BaseTrapSeverity=[INTEGER], BaseTrapProbableCause=[INTEGER], BaseTrapEventType=[INTEGER], EntPhysicalContainedIn=[INTEGER], EntPhysicalName=[OCTET], RelativeResource=[OCTET], ReasonDescription=[OCTET])

The transmit power of an optical module is too high.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800043	Minor	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
Index	Indicates the index.
EntityPhysicalIndex	Indicates the index of the physical entity.
PhysicalName	Indicates the name of the physical entity.
EntityTrapFaultID	Indicates the error code.

Name	Meaning
EntityTrapReasonDescr	Indicates the description of the alarm cause.

Impact on the System

This alarm does not affect system operating if the interface on which the optical module is installed works properly.

Possible Causes

The transmit power of the optical module is too high.

Procedure

- Step 1** Run the **display transceiver slot *slot-id* verbose** command in the system view to check whether the transmit power **Tx Power** of the optical module is within the allowed range.
- If so, services are not affected. Collect alarms, logs, and configurations and contact technical support personnel.
 - If not, go to step 2.
- Step 2** Check whether the transmit power upper threshold of the optical module is within the acceptable range.
- If so, run the **transceiver diagnosis threshold tx-power** command to change the transmit power upper threshold of the optical module. The alarm handling ends.
 - If not, go to step 3.
- Step 3** Use an optical attenuator to reduce the transmit power of the optical module to the acceptable range. Check whether the alarm is cleared.
- If so, the alarm handling ends.
 - If not, go to step 4.
- Step 4** Replace the optical module, and check whether the alarm is cleared.
- If so, the alarm handling ends.
 - If not, collect alarms, logs, and configurations, and contact technical support personnel.

----End

Related Information

None

3.3.62.2 ALM-3276800043 Indicates that the optical power exceeds the upper alarm threshold or falls below the lower alarm threshold 136194

Description

SRM/3/TXPOWER_EXCEEDMINOR: OID [OID] Optical module exception, Tx power is too low. (EntityPhysicalIndex=[INTEGER], BaseTrapSeverity=[INTEGER], BaseTrapProbableCause=[INTEGER], BaseTrapEventType=[INTEGER], EntPhysicalContainedIn=[INTEGER], EntPhysicalName=[OCTET], RelativeResource=[OCTET], ReasonDescription=[OCTET])

The transmit power of an optical module is too low.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800043	Minor	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
Index	Indicates the index.
EntityPhysicalIndex	Indicates the index of the physical entity.
PhysicalName	Indicates the name of the physical entity.
EntityTrapFaultID	Indicates the error code.
EntityTrapReasonDescr	Indicates the description of the alarm cause.

Impact on the System

This alarm does not affect system operating if the interface on which the optical module is installed works properly.

Possible Causes

The transmit power of the optical module is too low.

Procedure

- Step 1** Run the **display transceiver slot *slot-id* verbose** command in the system view to check whether the transmit power **Tx Power** of the optical module is within the allowed range.
- If so, services are not affected. Collect alarms, logs, and configurations and contact technical support personnel.
 - If not, go to step 2.
- Step 2** Check whether the transmit power lower threshold of the optical module is within the acceptable range.
- If so, run the **transceiver diagnosis threshold tx-power** command to change the transmit power lower threshold of the optical module. The alarm handling ends.
 - If not, go to step 3.
- Step 3** Replace the optical module, and check whether the alarm is cleared.
- If so, the alarm handling ends.
 - If not, collect alarms, logs, and configurations, and contact technical support personnel.

----End

Related Information

None

3.3.62.3 ALM-3276800043 Indicates that the optical power exceeds the upper alarm threshold or falls below the lower alarm threshold 136195

Description

SRM/3/RXPOWER_EXCEEDMAJOR: OID [OID] Optical module exception, Rx power is too high. (EntityPhysicalIndex=[INTEGER], BaseTrapSeverity=[INTEGER], BaseTrapProbableCause=[INTEGER], BaseTrapEventType=[INTEGER], EntPhysicalContainedIn=[INTEGER], EntPhysicalName=[OCTET], RelativeResource=[OCTET], ReasonDescription=[OCTET])

The receive power of an optical module is too high.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800043	Minor	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
Index	Indicates the index.
EntityPhysicalIndex	Indicates the index of the physical entity.
PhysicalName	Indicates the name of the physical entity.
EntityTrapFaultID	Indicates the error code.
136195	Indicates that the receive power of the optical module is too high.
EntityTrapReasonDescr	Indicates the description of the alarm cause.

Impact on the System

This alarm does not affect system operating if the interface on which the optical module is installed works properly.

Possible Causes

The receive power is too high.

Procedure

- Step 1** Run the **display transceiver slot *slot-id* verbose** command in the system view to check whether the receive power **Rx Power** of the optical module is within the allowed range.
- If so, collect alarms, logs, and configurations, and contact technical support personnel.
 - If not, go to step 2.
- Step 2** Check whether the receive power of the optical module is within a usable range.
- If so, run the **transceiver diagnosis threshold rx-power** command to change the receive power upper threshold of the optical module. The alarm handling ends.
 - If not, go to step 3.
- Step 3** Check whether an alarm is generated for high transmit power on the peer optical module. If so, rectify the peer optical module fault first.
- Step 4** Check whether the peer optical module and the local optical module are of the same type. If not, replace the local optical module with a new one to ensure they are of the same type.

- Step 5** Add -5 dBm (recommended) attenuators to the optical module.
- Step 6** If the problem persists after the preceding steps, collect alarms, logs, and configurations, and contact technical support personnel.
- End

Related Information

None

3.3.62.4 ALM-3276800043 Indicates that the optical power exceeds the upper alarm threshold or falls below the lower alarm threshold 136196

Description

SRM/3/RXPOWER_EXCEEDMINOR: OID [OID] Optical module exception, Rx power is too low. (EntityPhysicalIndex=[INTEGER], BaseTrapSeverity=[INTEGER], BaseTrapProbableCause=[INTEGER], BaseTrapEventType=[INTEGER], EntPhysicalContainedIn=[INTEGER], EntPhysicalName=[OCTET], RelativeResource=[OCTET], ReasonDescription=[OCTET])

The receive power of an optical module is too low.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800043	Minor	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
Index	Indicates the index.
EntityPhysicalIndex	Indicates the index of the physical entity.
PhysicalName	Indicates the name of the physical entity.
EntityTrapFaultID	Indicates the error code.
EntityTrapReasonDescr	Indicates the description of the alarm cause.

Impact on the System

This alarm does not affect system operating if the interface on which the optical module is installed works properly.

Possible Causes

The receive power of the optical module was too low.

Procedure

- Step 1** Run the **display transceiver slot *slot-id* verbose** command in the system view to check whether the receive power **Rx Power** of the local interface is within the acceptable range.
- If so, collect alarms, logs, and configurations, and contact technical support personnel.
 - If not, go to step 2.
- Step 2** Check whether the receive power of the optical module is within a usable range.
- If so, run the **transceiver diagnosis threshold rx-power** command to change the receive power lower threshold of the optical module. The alarm handling ends.
 - If not, go to step 3.
- Step 3** Check whether the peer port is physically Up and whether there is no alarm indicating that the transmit power is too low.
- If so, perform an external loopback test on the interface. If the interface is in Up state, perform loopback tests on the nodes along the transmission path to locate the failure point or link. Then check whether the alarm is cleared. If not, go to 4.
 - If not, go to step 4.
- Step 4** Check whether the peer port is physically Down and a corresponding alarm is generated, rectify the fault on the peer port.
- If so, repair the peer port. Check whether the alarm is cleared. If not, go to step 5.
 - If not, go to step 5.
- Step 5** Test whether the fiber is working normally.
- If so, replace the fiber and check whether the alarm is cleared. If not, go to step 6.
 - If not, go to step 6.
- Step 6** Replace the optical module of the local port and check whether the alarm is cleared.
- If so, the alarm handling ends.
 - If not, go to step 7.
- Step 7** Collect alarms, logs, and configurations, and contact technical support personnel.

----End

Related Information

None

3.3.63 ALM-3276800044 An Optical Module Installed on the Device Is Not a Huawei-Certified Optical Module

Description

ENTITYTRAP/3/OPTICALUNAUTHORIZED: OID [OID] The optical module was not certified by Huawei Ethernet Switch. (Index=[INTEGER], EntityPhysicalIndex=[INTEGER], PhysicalName="[OCTET]", EntityTrapFaultID=[INTEGER], EntityTrapReasonDescr="[OCTET]")

An optical module installed on the device is not a Huawei-certified optical module.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800044	Minor	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
Index	Indicates the index.
EntityPhysicalIndex	Indicates the index of the physical entity.
PhysicalName	Indicates the entity name.
EntityTrapFaultID	Indicates the error code.
EntityTrapReasonDescr	Indicates the reason description of the alarm.

Impact on the System

See the description in the procedure.

Possible Causes

- Cause 1: The optical module is not a Huawei-customized optical module. If this optical module was delivered from Huawei early.

- Cause 2: Temperature of the installed optical module did not conform to the temperature specifications of the switch-supported optical module. The corresponding port may become Down.

Procedure

- Cause 1: The optical module is not a Huawei-customized optical module. If this optical module was delivered from Huawei early.
 - a. If this optical module was delivered from Huawei earlier, run the **transceiver phony-alarm-disable** command to disable the alarm function for non-Huawei customized optical modules.
 - b. If this optical module is not delivered from Huawei or is not customized for Huawei, replace it with a Huawei-customized optical module.
- Cause 2: Temperature of the installed optical module did not conform to the temperature specifications of the switch-supported optical module. The corresponding port may become Down.

Replace the optical module with a switch-supported optical module. For switch support for optical modules, see "Appearance and Structure" in the *Hardware Description*.

Related Information

None

3.3.64 ALM-3276800045 Indicates that the board ports conflict with each other

3.3.64.1 ALM-3276800045 Indicates that the board ports conflict with each other 147456

Description

ENTITYTRAP/4/PORTCONFLICT: OID [OID] Some ports on the board and subcard conflict with each other. (Index=[INTEGER], EntityPhysicalIndex=[INTEGER], PhysicalName="[OCTET]", EntityTrapEntType=[INTEGER], EntityTrapFaultID=[INTEGER], EntityTrapReasonDescr="[OCTET]")

The switch worked in card interface working mode, but no card was installed.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800045	Warning	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
Index	Index.
EntityPhysicalIndex	Physical index.
PhysicalName	Entity name.
EntityTrapEntType	Entity type.
EntityTrapFaultID	Error code 147456.
EntityTrapReasonDescr	Cause of the alarm.

Impact on the System

The four 10GE SFP+ Ethernet optical interfaces on the front panel could not be used.

Possible Causes

The switch worked in card interface working mode, but no card was installed.

Procedure

Install a card supported by the switch.

3.3.64.2 ALM-3276800045 Indicates that the board ports conflict with each other 147457

Description

ENTITYTRAP/4/PORTCONFLICT: OID [OID] Some ports on the board and subcard conflict with each other. (Index=[INTEGER], EntityPhysicalIndex=[INTEGER], PhysicalName="[OCTET]", EntityTrapEntType=[INTEGER], EntityTrapFaultID=[INTEGER], EntityTrapReasonDescr="[OCTET]")

The switch worked in panel interface working mode, but the card on the switch was not removed.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800045	Warning	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
Index	Index.
EntityPhysicalIndex	Physical index.
PhysicalName	Entity name.
EntityTrapEntType	Entity type.
EntityTrapFaultID	Error code 147457.
EntityTrapReasonDescr	Cause of the alarm.

Impact on the System

None

Possible Causes

The switch worked in panel interface working mode, but the card on the switch was not removed.

Procedure

Remove the card on the switch.

3.3.65 ALM-3276800046 Station author is error notify

Description

WLAN/4/STA_AUTH_FAIL: OID [oid] Station author is error notify.
 (APMAC=[OPAQUE],APMAC=[OPAQUE],RadioID=[INTEGER],StaMac=[OPAQUE],APName=[OCTET],StaAssocBssid=[OPAQUE],Ssid=[OCTET],StaAuthenticationMode=[INTEGER],StaFailCodeType=[OCTET],StaAuthenticationFailCause=[INTEGER],StaAuthenticationFailCauseStr=[OCTET], APID=[INTEGER])

A STA failed to be authenticated.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800046	Warning	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
APMAC	Indicates the MAC address of an AP.
RadioID	Indicates the radio ID.
StaMac	Indicates the MAC address of a STA, which identifies the STA and functions as the index for querying information associated with the STA.
APName	Indicates the AP name.
StaAssocBssid	Indicates the BSSID associated with the STA.
Ssid	Indicates the SSID associated with the STA.
StaAuthenticationMode	Indicates the authentication mode of the STA.
StaFailCodeType	Indicates the code type of failures of STA authentication and association. • 1: Reason code • 2: Status code
StaAuthenticationFailCause	Indicates the index of the authentication failure reason.
StaAuthenticationFailCauseStr	Indicates the user authentication failure reason.
APID	Indicates the AP ID.

Impact on the System

STAs cannot go online.

Possible Causes

The AP was configured with the WEP shared key authentication mode and the STA sent a connection request with an incorrect password.

Procedure

- Step 1** Check whether the shared key is configured correctly.
- If so, go to Step 2.

- If not, this is a common event. Go to step 3.

Step 2 Collect alarm messages, log messages, and configurations, and then contact the technical support personnel.

Step 3 End.

----End

Related Information

None

3.3.66 ALM-3276800047 Patch deleted needs restart trap

Description

SSPADP/4/PATCHDELNEEDREST: OID [OID] The device needs to restart after the patch is deleted.

The switch needs to be restarted after the patch is deleted.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800047	Warning	environmentalAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.

Impact on the System

The switch needs to be restarted.

Possible Causes

The patch in the system is deleted.

Procedure

After the patch is deleted, restart the switch.

3.3.67 ALM-3276800048 Input flow bandwidth usage exceeded the threshold

Description

ENTITYEXTTRAP/2/INUSAGEEXCEED: OID [OID] Input flow bandwidth usage exceeded the threshold. (SlotID=[STRING], UnitID=[INTEGER], PortID=[STRING], PeerSlotID=[STRING], CurUsage=[INTEGER], Threshold=[INTEGER])

The inbound bandwidth on the stack link exceeds the alarm threshold.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800048	Major	Quality of service alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
SlotID	Indicates the slot ID.
UnitID	Indicates the chip ID. The value 65535 indicates that the value is meaningless.
PortID	Indicates the port name of the stack link.
PeerSlotID	Indicates the slot ID of the peer device.
CurUsage	Indicates the current bandwidth usage. If the current bandwidth usage cannot be obtained, it displays 0.
Threshold	Indicates the bandwidth usage alarm threshold.

Impact on the System

The stack link may be congested.

Possible Causes

The inbound bandwidth usage of the stack link exceeds the alarm threshold.

Procedure

Collect alarm information and configuration information, and then contact technical support personnel.

Related Information

None

3.3.68 ALM-3276800049 VAP has the max number of stations notify

Description

WLAN/4/VAP_REACH_MAX_USERS:OID [OID] VAP has the max number of stations notify.(APMAC=[OPAQUE], APName=[STRING], RADIOID=[INTEGER], WLANID=[INTEGER], FailCause=[INTEGER], PermitNum=[INTEGER], APID=[INTEGER])

No station (STA) can be associated with the VAP.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800049	Warning	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
APMAC	Indicates the MAC address of an AP.
APName	Indicates the AP name.
RADIOID	Indicates the radio ID of the AP.
WLANID	Indicates the WLAN ID reporting the alarm.
FailCause	Indicates the cause for the STA authentication failure.
PermitNum	Indicates the maximum number of STAs that can be associated with the AP.
APID	Indicates the AP ID.

Impact on the System

New STAs cannot connect to the VAP.

Possible Causes

The number of STAs connected to the VAP has reached the upper limit. New STAs cannot connect to the VAP.

Procedure

- Step 1** Check whether the maximum number of STAs allowed to connect to the SSID is proper.
- If so, go to Step 3.
 - If not, go to Step 2.
- Step 2** In the SSID profile, run the **max-sta-number** *max-sta-number* command to change the maximum number of STAs allowed to connect to the SSID to a proper value. Check whether the alarm persists.
- If so, go to Step 3.
 - If not, go to Step 5.
- Step 3** The VAP cannot provide WLAN services to STAs. Associate new STAs to another VAP. Then, check whether the alarm persists.
- If so, go to Step 4.
 - If not, go to Step 5.
- Step 4** Collect alarm messages, log messages, and configurations, and then contact the technical support personnel.
- Step 5** End.

----End

Related Information

None

3.3.69 ALM-3276800050 Output flow bandwidth usage exceeded the threshold

Description

ENTITYEXTTRAP/2/OUTUSAGEEXCEED: OID [OID] Output flow bandwidth usage exceeded the threshold. (SlotID=[STRING], UnitID=[INTEGER], PortID=[STRING], PeerSlotID=[STRING], CurUsage=[INTEGER], Threshold=[INTEGER])

The outbound bandwidth usage on the stack link exceeds the alarm threshold.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800050	Major	Quality of service alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
SlotID	Indicates the slot ID.
UnitID	Indicates the chip ID. The value 65535 indicates that the value is meaningless.
PortID	Indicates the port name of the stack link.
PeerSlotID	Indicates the slot ID of the peer device.
CurUsage	Indicates the current bandwidth usage.
Threshold	Indicates the bandwidth usage alarm threshold.

Impact on the System

The stack link may be congested.

Possible Causes

The outbound bandwidth usage of the stack link exceeds the alarm threshold.

Procedure

Collect alarm information and configuration information, and then contact technical support personnel.

Related Information

None

3.3.70 ALM-3276800052 Packets are discarded for an error

Description

ENTITYEXTTRAP/2/PKTERRORRISING: OID [OID] Input packets are discarded for an error in physical layer detection. (SlotID=[STRING], UnitID=[INTEGER],

PortID=[STRING], PeerSlotID=[STRING], ErrorPacketStatistics=[STRING],
ErrorPacketThreshold=[STRING], MonitorInterval=[STRING])

The total number of error packets on an HG channel or stack port exceeds the alarm threshold.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800052	Major	Communication alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
SlotID	Indicates the slot ID.
UnitID	Indicates the chip ID. NOTE The value is 0 or 1 for the HG channel or 65535 (an invalid value) for a stack port.
PortID	Indicates the port number of the HG channel or stack port.
PeerSlotID	Indicates the slot ID of the remote card.
ErrorPacketStatistics	Indicates the total number of error packets.
ErrorPacketThreshold	Alarm threshold for error packets.
MonitorInterval	Indicates the detection interval.

Impact on the System

The HG channel or stack port cannot forward packets normally. During inter-card or inter-device traffic forwarding, packets are lost or cannot be forwarded.

Possible Causes

The device is faulty.

Procedure

Replace the device.

Related Information

[3.3.71 ALM-3276800053 Higig port state has changed](#)

[3.3.72 ALM-3276800054 Port state is always down](#)

3.3.71 ALM-3276800053 Higig port state has changed

Description

ENTITYEXTTRAP/2/HGSTATECHANGE: OID [OID] Higig port state has changed. (SlotID=[STRING], UnitID=[INTEGER], PortID=[STRING], PeerSlotID=[STRING], ChangedTimes=[STRING])

The HG channel state has changed.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800053	Major	Communication alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
SlotID	Indicates the slot ID.
UnitID	Indicates the chip ID.
PortID	Indicates the port number of the HG channel.
PeerSlotID	Indicates the slot ID of the remote card.
ChangedTimes	Indicates the number of times the HG channel state has changed.

Impact on the System

The HG channel cannot forward packets normally. During inter-card traffic forwarding, packets are lost or cannot be forwarded.

Possible Causes

The device is faulty.

Procedure

Replace the device.

Related Information

[3.3.70 ALM-3276800052 Packets are discarded for an error](#)

[3.3.72 ALM-3276800054 Port state is always down](#)

3.3.72 ALM-3276800054 Port state is always down

Description

ENTITYEXTTRAP/2/HGSTATEDOWN: OID [OID] Higi port state is always DOWN.
 (SlotID=[STRING], UnitID=[INTEGER], PortID=[STRING], PeerSlotID=[STRING],
 MonitorInterval=[STRING])

The HG channel state remains Down.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800054	Major	Communication alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
SlotID	Indicates the slot ID.
UnitID	Indicates the chip ID.
PortID	Indicates the port number of the HG channel.
PeerSlotID	Indicates the slot ID of the remote card.
MonitorInterval	Indicates the detection interval.

Impact on the System

The HG channel cannot forward packets normally. During inter-card traffic forwarding, packets are lost or cannot be forwarded.

Possible Causes

The device is faulty.

Procedure

Replace the device.

Related Information

[3.3.70 ALM-3276800052 Packets are discarded for an error](#)

[3.3.72 ALM-3276800054 Port state is always down](#)

3.3.73 ALM-3276800055 Discards the runt packets

Description

ENTITYEXTTRAP/4/RUNTPKTDROP: OID [OID] The board has been detected that discards the runt packets, which may affect services. (PhysicalIndex=[INTEGER], PhysicalName=[OCTET], BoardDroppedRuntPkt=[COUNTER64], TimeInterval=[INTEGER])

An alarm is generated when some packets of 64 to 86 bytes or 145 to 193 bytes, which are forwarded by the card at the line rate, are lost.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800055	Warning	Quality of service alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
PhysicalIndex	Indicates the index of a card.
PhysicalName	Indicates the name of a card.
BoardDroppedRuntPkt	Indicates the number of dropped packets.
TimeInterval	Indicates the interval at which statistics about dropped packets are collected.

Impact on the System

Packet loss will occur when packets of 64 to 86 bytes or 145 to 193 bytes are forwarded at the line rate.

Possible Causes

The cards forward a high volume of traffic.

Procedure

Expand the capacity or load balance the traffic to reduce the traffic forwarded by the card.

Related Information

None

3.3.74 ALM-3276800056 The bridge loses the position of root bridge

Description

MSTP/4/PROROOTLOST: OID [OID] The bridge loses the position of root bridge. (ProcessID=[ProcessID], InstanceID=[InstanceID])

The device in an MSTP process lost its root bridge role.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800056	Warning	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
ProcessID	Process ID.
InstanceID	Instance ID.

Impact on the System

The network topology will be changed, and traffic will be forwarded through a new path.

Possible Causes

After a root bridge was specified using the **stp [instance *instance-id*] root primary** command in the MSTP process or system view, a device whose priority changed to 0 became the new root bridge.

NOTE

This alarm is not triggered in an instance with a non-zero ID of a process with a non-zero ID.

Procedure

- Step 1** View physical devices on the network and check whether a new STP-enabled physical link is added to the topology.
- If such a link is added, go to Step 2.
 - If no such link is added, go to Step 5.
- Step 2** Check whether the added physical link is the required one.
- If the link is required, go to Step 3.
 - If the link is not required, go to Step 9.
- Step 3** Run the **display stp [process *process-id*] [instance *instance-id*] [interface *interface-type interface-number* | slot *slot-id*] [brief]** command to check whether the added device is the root bridge.
- If the device is the root bridge, go to Step 4.
 - If the device is not the root bridge, go to Step 5.
- Step 4** Check whether the priority of the added device is proper.
- If the priority is proper, go to Step 8.
 - If the priority is improper, go to Step 9.
- Step 5** Run the **display stp [process *process-id*] [instance *instance-id*] [interface *interface-type interface-number* | slot *slot-id*] [brief]** command to check whether a device's priority is changed in the network topology.
- If a device's priority is changed, go to Step 6.
 - If no device's priority is changed, go to Step 10.
- Step 6** Check whether the priority modification is proper.
- If the modification is proper, go to Step 8.
 - If the modification is improper, go to Step 7.
- Step 7** Run the **stp [instance *instance-id*] priority *priority*** command in the system view or MSTP process view of the device whose priority has been changed to re-set its priority as needed. Alternatively, run the **undo stp [instance *instance-id*] priority** or **undo stp [instance *instance-id*] root** command to restore the default priority. Check whether the alarm is cleared.
- If the alarm is cleared, go to Step 11.
 - If the alarm persists, go to Step 9.
- Step 8** Run the **undo stp [instance *instance-id*] root** command in the system view or MSTP process view of the device that has lost the root bridge role. Then check whether the alarm is cleared.

- If the alarm is cleared, go to Step 11.
- If the alarm persists, go to Step 10.

Step 9 Correct the network topology and check whether the alarm is cleared.

- If the alarm is cleared, go to Step 11.
- If the alarm persists, go to Step 10.

Step 10 Collect alarm information and configuration information, and then contact technical support personnel.

Step 11 End.

----End

Related Information

None

3.3.75 ALM-3276800057 Station association is failed notify

Description

WLAN/4/STA_ASSOCIATION_FAIL: OID [OID] Station association is failed notify. (APMAC=[OPAQUE],APMAC=[OPAQUE],RadioID=[INTEGER],StaMac=[OPAQUE],APName=[OCTET],StaAssocBssid=[OPAQUE],Ssid=[OCTET],StaFailCodeType=[OCTET],StaAuthenticationFailCause=[INTEGER], StaAssociationFailCauseStr=[OCTET], APID=[INTEGER])

A STA failed to associate with the AP.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800057	Warning	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
APMAC	Indicates the MAC address of an AP.
RadioID	Indicates the radio ID.
StaMac	Indicates the MAC address of a STA, which identifies the STA and functions as the index for querying information associated with the STA.

Name	Meaning
APName	Indicates the AP name.
StaAssocBssid	Indicates the BSSID associated with the STA.
Ssid	Indicates the SSID associated with the STA.
StaAuthenticationMode	Indicates the authentication mode of the STA.
StaFailCodeType	Indicates the code type of failures of STA authentication and association. • 1: Reason code • 2: Status code
StaAuthenticationFailCause	Indicates the index of the authentication failure reason.
StaAuthenticationFailCauseStr	Indicates the user authentication failure reason.
APID	Indicates the AP ID.

Impact on the System

STAs cannot go online.

Possible Causes

The number of STAs that send association requests to the AP exceeded the maximum value allowed by the AP.

Procedure

- Step 1** Run the **display sta-blacklist-profile** command to check whether the STA is in the specified STA blacklist profile.
- If so, go to Step 2.
 - If not, go to Step 3.
- Step 2** Run the **undo sta-mac** command to delete the STA from the blacklist. Check whether the alarm persists.
- If so, go to Step 3.
 - If not, go to Step 6.
- Step 3** Check whether the number of STAs has reached the allowed maximum value.
- If so, go to Step 4.
 - If not, go to Step 5.

- Step 4** Associate STAs with other APs. Check whether the alarm persists.
- If so, go to Step 5.
 - If not, go to Step 6.
- Step 5** Collect alarm messages, log messages, and configurations, and then contact the technical support personnel.
- Step 6** End.
- End

Related Information

None

3.3.76 ALM-3276800058 The port works in half duplex mode

Description

SRM/4/HALFDUPLEXALARM: OID [OID] The port works in half duplex mode.
(EntityPhysicalIndex=[INTEGER1], BaseTrapSeverity=[INTEGER2],
BaseTrapProbableCause=[INTEGER3], BaseTrapEventType=[INTEGER4],
EntPhysicalName=[OCTET1], RelativeResource=[OCTET2])

This alarm was generated when the Ethernet interface worked in half-duplex mode.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800058	Warning	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
[INTEGER1]	Entity index.
[INTEGER2]	Severity code.
[INTEGER3]	Error code.
[INTEGER4]	Code of the event type.
[OCTET1]	Entity name.
[OCTET2]	Name of the affected component.

Impact on the System

It may result in packet loss, low bandwidth usage, or even network interruption.

Possible Causes

1. The local interface or the peer interface was configured to work in half-duplex mode.
2. One of the connected interfaces worked in auto-negotiation mode whereas the other interface worked in non-automatic negotiation mode.

Procedure

- Step 1** Check whether the interface is expected to work in half-duplex mode.
- (1) If so, go to Step 5.
 - (2) If not, go to Step 2.
- Step 2** In the interface view of the local interface and the peer interface, run the **display this** command to check whether the half-duplex mode is configured.
- (1) If so, run the **duplex full** command to forcibly configure the interface to work in full-duplex mode.
 - (2) If not, go to Step 4.
- Step 3** In the interface view of the local interface and the peer interface, run the **display this** command to check whether one interface works in auto-negotiation mode whereas the other interface works in non-automatic negotiation mode.
- (1) If so, run the **negotiation auto** command to configure the interface working in non-automatic negotiation mode to work in auto-negotiation mode.
 - (2) If not, go to Step 4.
- Step 4** Contact technical support personnel.
- Step 5** End.
- End

Related Information

None

3.3.77 ALM-3276800059 The port works in full duplex mode

Description

SRM/4/HALFDUPLEXCLEAR: OID [OID] The port works in full duplex mode.
(EntityPhysicalIndex=[INTEGER], BaseTrapSeverity=[INTEGER],
BaseTrapProbableCause=[INTEGER], BaseTrapEventType=[INTEGER],
EntPhysicalName=[OCTET],RelativeResource=[OCTET])

The interface working mode changed to full duplex.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800059	Warning	Communication alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
EntityPhysicalIndex	Indicates the interface index.
BaseTrapSeverity	Indicates the alarm severity.
BaseTrapProbableCause	Indicates the alarm cause.
BaseTrapEventType	Indicates the alarm type.
EntPhysicalName	Indicates the interface name.
RelativeResource	Indicates the relative resource.

Impact on the System

The interface alternates between Up and Down states.

Possible Causes

The interface begins to work in half duplex mode. When the interface works in full duplex mode, a full duplex alarm is generated.

Procedure

Step 1 Check whether the duplex state of the interface is correct according to networking requirements.

Run the **display interface** *interface-type* [*interface-number*] command to check the duplex state of the interface.

- If the duplex state of the interface is incorrect, modify the interface configuration.
- If the duplex state of the interface is correct, go to step 2.

Step 2 End.

----End

Related Information

[3.3.76 ALM-3276800058 The port works in half duplex mode](#)

3.3.78 ALM-3276800060 Physical entity port type changed

Description

SRM/3/PortPhysicalPortTypeChange: OID [OID] port type changed.
(EntityPhysicalIndex=[INTEGER], BaseTrapSeverity=[INTEGER],
BaseTrapProbableCause=[INTEGER], BaseTrapEventType=[INTEGER],
EntPhysicalName=[OCTET], BaseTrapLastPortType=[INTEGER],
BaseTrapCurPortType=[INTEGER])

The interface media type changed.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800060	Minor	operationalViolation(8)

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
EntityPhysicalIndex	Indicates the interface index.
BaseTrapSeverity	Indicates the alarm severity.
BaseTrapProbableCause	Indicates the alarm cause.
BaseTrapEventType	Indicates the alarm type.
EntPhysicalName	Indicates the interface name.
BaseTrapLastPortType	Indicates the previous media type.
BaseTrapCurPortType	Indicates the current media type.

Impact on the System

The optical module or cable needs to be replaced.

Possible Causes

The working mode of the combo interface was changed.

Procedure

This alarm is informational only, and no action is required.

Related Information

None

3.3.79 ALM-3276800061 ACL resource is full

Description

ACLE/4/ACL_RULERESFULL_TRAP:OID [OID] The rule resource usage has reached [INTEGER]%. (Slot=[OCTET], Stage=[OCTET])

The ACL resource usage reaches 100%.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800061	Warning	Quality of service alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
INTEGER	The value is fixed as 100%.
Slot	Specifies the stack ID of the card where the alarm is generated.
Stage	Indicates the ACL processing stage when the alarm is generated.

Impact on the System

None

Possible Causes

The ACL resource usage reaches 100%.

Procedure

Step 1 Run the **display acl resource slot** [*slot-id*] command in the system view to check whether the ACL resource usage on the switch is the same as the value in alarm.

- If so, go to step 2.
- If not, go to step 3.

Step 2 The following are suggestions:

- Check whether global or simplified traffic policy can be disabled on the device. If so, change the global or simplified traffic policy into interface-based traffic policy.
- Replace the boards with the boards that provide more ACL resources.

After the operation, check whether the alarm is cleared.

- If so, go to step 4.
- If not, go to step 3.

Step 3 Collect alarm, log, and configuration information, and contact technical support personnel.

Step 4 End.

----End

Related Information

None

3.3.80 ALM-3276800062 Tamper attack notify

Description

WLAN/4/STA_INVALID_CERT_ATTACK: OID [OID] User with invalid certificate inbreak network notify.
(APMAC=[OPAQUE],APMAC=[OPAQUE],RadioID=[INTEGER],StaMac=[OPAQUE],APName=[OCTET],StaAssocBssid=[OPAQUE],Ssid=[OCTET], APID=[INTEGER])

A user with an invalid certificate accessed the network.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800062	Warning	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
APMAC	Indicates the MAC address of an AP.
RadioID	Indicates the radio ID.
StaMac	Indicates the MAC address of a STA, which identifies the STA and functions as the index for querying information associated with the STA.

Name	Meaning
APName	Indicates the AP name.
StaAssocBssid	Indicates the BSSID associated with the STA.
Ssid	Indicates the SSID associated with the STA.
APID	Indicates the AP ID.

Impact on the System

STAs cannot go online.

Possible Causes

A user with an invalid WAPI certificate accessed the network.

Procedure

- Step 1** Run the **display wlan wapi certificate file-name** *file-name* command to check whether the WAPI certificate is correct.
- If so, go to Step 3.
 - If not, go to Step 2.
- Step 2** Run the **wapi import certificate { ac | asu | issuer } format pkcs12 file-name** *file-name* **password** *password* or **wapi import certificate { ac | asu | issuer } format pem file-name** *file-name* command to import a correct WAPI certificate. Check whether the alarm persists.
- If so, go to Step 3.
 - If not, go to Step 4.
- Step 3** Collect alarm messages, log messages, and configurations, and then contact the technical support personnel.
- Step 4** End.
- End

Related Information

None

3.3.81 ALM-3276800063 ACL resource lack

Description

ACLE/4/ACL_RULERESLACK_TRAP:OID [OID] The rule resource usage has exceeded [INTEGER]%. (Slot=[OCTET], Stage=[OCTET])

The ACL resource usage reaches the upper threshold.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800063	Warning	Quality of service alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
INTEGER	Indicates the upper threshold of ACL resource usage.
Slot	Specifies the stack ID of the card where the alarm is generated.
Stage	Indicates the ACL processing stage when the alarm is generated.

Impact on the System

None

Possible Causes

The ACL resource usage reaches the upper limit.

Procedure

- Step 1** Check whether the threshold of ACL resources is too low in the system view. By default, the lower threshold is 70% and the upper threshold is 80%. Users can specify the threshold range according to service requirements.
- If so, go to step 2.
 - If not, go to step 3.
- Step 2** Run the **acl threshold-alarm { upper-limit *upper-limit* | lower-limit *lower-limit* }** * command in the system view to reset the alarm thresholds. Check whether the alarm is cleared.
- If so, go to step 6.
 - If not, go to step 3.
- Step 3** Run the **display acl resource slot [*slot-id*]** command in the system view to check whether the ACL resource usage on the switch is the same as the value in alarm.
- If so, go to step 4.

- If not, go to step 5.

Step 4 The following are suggestions:

- Check whether global or simplified traffic policy can be disabled on the device. If so, change the global or simplified traffic policy into interface-based traffic policy.
- Replace the boards with the boards that provide more ACL resources.

After the operation, check whether the alarm is cleared.

- If so, go to step 6.
- If not, go to step 5.

Step 5 Collect alarm, log, and configuration information, and contact technical support personnel.

Step 6 End.

----End

Related Information

None

3.3.82 ALM-3276800064 The Layer 3 Resource Usage Reaches or Exceeds the Upper Threshold

Description

L3MB/4/FwdResLack:OID [OID] The layer 3 resource usage has reached or exceeded [Threshold]%.
(EntPhysicalIndex=[GAUGE],EntPhysicalName=[OCTET],Slot=[OCTET],ResourceType=[INTEGER])

The Layer 3 resource usage reaches or exceeds the upper threshold. Except the IPv4 route prefix entries, all Layer 3 resources have an upper usage threshold of 85%, which cannot be changed.

NOTE

You can use the **fib threshold-alarm** command to set the upper threshold of the IPv4 route prefix entries.

By default, the upper threshold of the IPv4 route prefix entries is 85%.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800064	Warning	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
Threshold	This object indicates the upper threshold of the layer 3 resource usage.
EntPhysicalindex	This object indicates the index of a physical entity.
EntPhysicalName	This object indicates the name of a physical entity.
Slot	This object indicates the slot ID.

Name	Meaning
ResourceType	This object indicates the ID of a Layer 3 resource. • hostTablePrefixTable(27) indicates the host route prefix entry. • routingTablePrefixTable(28) indicates the IPv4 route prefix entry. • ecmpNextHopTable(29) indicates the next hop entry of the equal-cost route. • layer3InterfaceTable(30) indicates the Layer 3 outbound interface entry. • nextHopTable(31) indicates the next hop entry. • tunnelDecapsulationTable(32) indicates the tunnel encapsulation and decapsulation entry. • ipv6RoutingTablePrefixTable(47) indicates the IPv6 route prefix entry. • ipv6DefipTable(767) indicates an IPv6 prefix entry of a route with a 128-bit mask. • tunnel6EncapsulationTable(742) indicates a IPv6 tunnel encapsulation and decapsulation entry. • tunnelEncapsulationTable(743) indicates a IPv4 tunnel encapsulation and decapsulation entry. • reTable(744) indicates a RE entry. • aibTable(745) indicates a AIB entry. • nstTable(746) indicates a NST entry. • vrrpTable(747) indicates a VRRP entry. • ipv6amTable(748) indicates a IPv6 AM entry.

Impact on the System

When the Layer 3 resource usage exceeds the upper threshold, services are not affected. If the usage of all Layer 3 resources reaches 100%, new Layer 3 services are unavailable.

Possible Causes

When the Layer 3 resource usage exceeds the upper threshold, an alarm is generated. When the usage reaches 100%, an alarm is generated again.

Procedure

Step 1 Lower the Layer 3 resource usage.

- Delete unnecessary host routes, and ND and ARP entries to release host route prefix resources.
- Delete unnecessary network segment routes to release IPv4 route prefix resources.
- Delete unnecessary equal-cost routes to release next hop resources.
- Delete unnecessary Layer 3 interfaces to release Layer 3 interface resources.
- Delete unnecessary routes including host routes and network segment routes, and ND and ARP entries to release next hop resources.
- Delete tunnels to release tunnel encapsulation and decapsulation resources.
- Delete unnecessary network segment routes to release IPv6 route IPv6 prefix entries.
- IPv6 prefix entries of routes with a 128-bit mask: Delete unnecessary network segment routes to release route prefix resources.
- IPv6 tunnel encapsulation and decapsulation entry: Delete IPv6 tunnels to release tunnel encapsulation and decapsulation resources.
- IPv4 tunnel encapsulation and decapsulation entry: Delete IPv4 tunnels to release tunnel encapsulation and decapsulation resources.
- RE entry: Delete unnecessary routes to release RE resources.
- AIB entry: Delete unnecessary ARP entries to release AIB resources.
- NST entry: Delete unnecessary ECMP routes to release NST resources.
- VRRP entry: Delete unnecessary VRRP configuration to release VRRP resources.
- IPv6 AM entry: Delete unnecessary IPv6 routes to release IPv6 AM resources.

Step 2 Collect the alarm information, log information, and configuration information, and then contact technical support personnel.

Step 3 End.

-----End

Related Information

None

3.3.83 ALM-3276800065 The STA Was Attacked by Replay Attacks

Description

WLAN/4/STA_REPLAY_ATTACK:OID [OID] Station repititive attack notify.
(APMAC=[OPAQUE],APMAC=[OPAQUE],RadioID=[INTEGER],StaMac=[OPAQUE],APName=[OCTET],StaAssocBssid=[OPAQUE],Ssid=[OCTET], APID=[INTEGER])

The STA was attacked by replay attacks.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800065	Warning	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
APMAC	Indicates the MAC address of an AP.
RadioID	Indicates the radio ID.
StaMac	Indicates the MAC address of a STA, which identifies the STA and functions as the index for querying information associated with the STA.
APName	Indicates the AP name.
StaAssocBssid	Indicates the BSSID associated with the STA.
Ssid	Indicates the SSID associated with the STA.
APID	Indicates the AP ID.

Impact on the System

STAs cannot go online.

Possible Causes

The AP received unauthorized AE questions.

Procedure

- Step 1** Check whether the MAC address of the STA is the same as that of the attack device.
- If so, go to Step 2.
 - If not, go to Step 4.
- Step 2** Run the **sta-mac mac-address [description description]** command to add the attack device's MAC address to the blacklist in the STA blacklist profile view.
- Step 3** Check whether the alarm persists.
- If so, go to Step 4.
 - If not, go to Step 5.
- Step 4** Collect alarm messages, log messages, and configurations, and then contact the technical support personnel.
- Step 5** End.
- End

Related Information

None

3.3.84 ALM-3276800066 Tamper attack notify

Description

WLAN/4/STA_TAMPER_ATTACK: OID [OID] Tamper attack notify.
(APMAC=[OPAQUE],APMAC=[OPAQUE],RadioID=[INTEGER],StaMac=[OPAQUE],APName=[OCTET],StaAssocBssid=[OPAQUE],Ssid=[OCTET], APID=[INTEGER])

Attack messages were modified.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800066	Warning	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
APMAC	Indicates the MAC address of an AP.
RadioID	Indicates the radio ID.

Name	Meaning
StaMac	Indicates the MAC address of a STA, which identifies the STA and functions as the index for querying information associated with the STA.
APName	Indicates the AP name.
StaAssocBssid	Indicates the BSSID associated with the STA.
Ssid	Indicates the SSID associated with the STA.
APID	Indicates the AP ID.

Impact on the System

STAs cannot go online.

Possible Causes

The AP received incorrect message authentication codes.

Procedure

- Step 1** Check whether the MAC address of the STA is the same as that of the attack device.
- If so, go to Step 2.
 - If not, go to Step 4.
- Step 2** Run the **sta-mac mac-address [description description]** command to add the attack device's MAC address to the blacklist in the STA blacklist profile view.
- Step 3** Check whether the alarm persists.
- If so, go to Step 4.
 - If not, go to Step 5.
- Step 4** Collect alarm messages, log messages, and configurations, and then contact the technical support personnel.
- Step 5** End.
- End

Related Information

None

3.3.85 ALM-3276800067 The AP Security Level Was Lowered

Description

WLAN/4/STA_SECURITY_CLASS_LOW_ATTACK: OID [oid] Low safelevel attack notify.
(APMAC=[OPAQUE],APMAC=[OPAQUE],RadioID=[INTEGER],StaMac=[OPAQUE],APName=[OCTET],StaAssocBssid=[OPAQUE],Ssid=[OCTET], APID=[INTEGER])

The AP security level was lowered by attacks.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800067	Warning	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
APMAC	Indicates the MAC address of an AP.
RadioID	Indicates the radio ID.
StaMac	Indicates the MAC address of a STA, which identifies the STA and functions as the index for querying information associated with the STA.
APName	Indicates the AP name.
StaAssocBssid	Indicates the BSSID associated with the STA.
Ssid	Indicates the SSID associated with the STA.
APID	Indicates the AP ID.

Impact on the System

STAs cannot go online.

Possible Causes

The AP received key negotiation response packets with incorrect WIEASUE.

Procedure

- Step 1** Check whether the MAC address of the STA is the same as that of the attack device.
- If so, go to Step 2.
 - If not, go to Step 4.
- Step 2** Run the **sta-mac mac-address [description description]** command to add the attack device's MAC address to the blacklist in the STA blacklist profile view.
- Step 3** Check whether the alarm persists.
- If so, go to Step 4.
 - If not, go to Step 5.
- Step 4** Collect alarm messages, log messages, and configurations, and then contact the technical support personnel.
- Step 5** End.
- End

Related Information

None

3.3.86 ALM-3276800068 Address redirection attack notify

Description

WLAN/4/STA_ADDRESS_REDIRCET_ATTACK:OID [OID] Address redirection attack notify.
(APMAC=[OPAQUE],APMAC=[OPAQUE],RadioID=[INTEGER],StaMac=[OPAQUE],APName=[OCTET],StaAssocBssid=[OPAQUE],Ssid=[OCTET], APID=[INTEGER])

An address redirection attack was detected.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800068	Warning	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
APMAC	Indicates the MAC address of an AP.
RadioID	Indicates the radio ID.

Name	Meaning
StaMac	Indicates the MAC address of a STA, which identifies the STA and functions as the index for querying information associated with the STA.
APName	Indicates the AP name.
StaAssocBssid	Indicates the BSSID associated with the STA.
Ssid	Indicates the SSID associated with the STA.
APID	Indicates the AP ID.

Impact on the System

STAs cannot go online.

Possible Causes

The AP received invalid WPI frames.

Procedure

- Step 1** Check whether the MAC address of the STA is the same as that of the attack device.
- If so, go to Step 2.
 - If not, go to Step 4.
- Step 2** Run the **sta-mac mac-address [description description]** command to add the attack device's MAC address to the blacklist in the STA blacklist profile view.
- Step 3** Check whether the alarm persists.
- If so, go to Step 4.
 - If not, go to Step 5.
- Step 4** Collect alarm messages, log messages, and configurations, and then contact the technical support personnel.
- Step 5** End.
- End

Related Information

None

3.3.87 ALM-3276800069 SSID WEP Key IDs Conflict

Description

WLAN/4/SSID_CONFLICT_WEP_KEY:OID [OID] SSID Wep key conflict notify.
(APMAC=[OPAQUE],WepIDConflictTrapAPMAC=[OPAQUE],WepIDConflictTrapAPName=[OCTET],WepIDConflictTrapRadioId=[INTEGER],WepIDConflictTrapPreSSID=[OCTET],WepIDConflictTrapCurrSSID=[OCTET],WepIDConflictTrapCipherIdx=[INTEGER], APID=[INTEGER])

WEP key ID collision has occurred.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800069	Warning	processingErrorAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
APMAC	Indicates the table index.
WepIDConflictTrapAPMAC	Indicates the MAC address of an AP.
WepIDConflictTrapAPName	Indicates the AP name.
WepIDConflictTrapRadioId	Indicates the radio ID configured on the AP when the collision happens.
WepIDConflictTrapPreSSID	Indicates the SSID configured before the collision.
WepIDConflictTrapCurrSSID	Indicates the SSID configured when the collision happens.
WepIDConflictTrapCipherIdx	Indicates the WEP key ID that causes the collision.
APID	Indicates the AP ID.

Impact on the System

Users fail to go online.

Possible Causes

Different WEP key IDs are configured in the security profiles bound to different VAPs.

Procedure

- Step 1** Run the **wep key** command to change **key-id** in the security profiles.
- If the alarm persists, go to Step 2.
 - If the alarm is cleared, go to Step 3.
- Step 2** Collect alarm messages, log messages, and configurations, and then contact the technical support personnel.
- Step 3** End.
- End

Related Information

None

3.3.88 ALM-3276800070 The Number of Users Associated with the AP Exceeds the Alarm Threshold

Description

WLAN/4/STA_NUM_EXCEED_THRESHOLD:OID [OID] AP access user number exceed threshold notify. (APMAC=[OPAQUE], RadioID=[INTEGER], APName=[OCTET], UserNum=[INTEGER], APID=[INTEGER])

The AP generates the alarm when the number of users associated with the AP exceeds the alarm threshold.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800070	Warning	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
ApMac	Indicates the MAC address of an AP.
APName	Indicates the AP name.
RadioID	Indicates the radio ID of the AP.

Name	Meaning
UserNum	Indicates the number of UAC users.
APID	Indicates the AP ID.

Impact on the System

When the number of users on a radio reaches the CAC threshold, the AP reports an alarm and denies access from new users. Since the system has other radios to provide services, user services will not be affected unless the number of users has exceeded the system capacity.

Possible Causes

The number of users associated with the AP radio has reached the upper limit and new users are associating with the AP radio.

Procedure

- Step 1** Run the **uac client-number threshold threshold access** *access-threshold* [**roam** *roam-threshold*] command in the RRM profile view to increase the upper limit on the number of users. Then, check whether the alarm persists.
- If so, go to Step 2.
 - If not, go to Step 3.
- Step 2** Collect alarm messages, log messages, and configurations, and then contact the technical support personnel.
- Step 3** End.
- End

Related Information

[3.3.89 ALM-3276800071 AP roam user number exceed threshold notify](#)

3.3.89 ALM-3276800071 AP roam user number exceed threshold notify

Description

WLAN/4/ROAM_STA_NUM_EXCEED_THRESHOLD:OID [OID] AP roam user number exceed threshold notify. (APMAC=[OPAQUE], RadioID=[INTEGER], APName=[OCTET], UserNum=[INTEGER], APID=[INTEGER])

The AP generates the alarm when the number of roaming users exceeds the alarm threshold.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800071	Warning	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
APMAC	Indicates the MAC address of an AP.
RadioID	Indicates the radio ID of the AP.
APName	Indicates the AP name.
UserNum	Indicates the number of UAC users.
APID	Indicates the AP ID.

Impact on the System

New users cannot roam to the AP.

Possible Causes

The number of roaming users on the AP exceeds the alarm threshold.

Procedure

Step 1 Run the **uac client-number threshold threshold access** *access-threshold* [**roam** *roam-threshold*] command in the radio profile view to increase the upper limit on the number of roaming users. Then, check whether the alarm persists.

- If so, go to Step 2.
- If not, go to Step 3.

Step 2 Collect alarm messages, log messages, and configurations, and then contact the technical support personnel.

Step 3 End.

----End

Related Information

None

3.3.90 ALM-3276800072 AP Access Channel Usage Exceeds the Threshold

Description

WLAN/4/CHANNEL_UTIL_EXCEED_THRESHOLD:OID [OID] AP access channelutilization exceed threshold notify. (APMAC=[OPAQUE], RadioID=[INTEGER], APName=[OCTET],ChannelUtil=[INTEGER], APID=[INTEGER])

The AP generates the alarm when the channel usage exceeds the alarm threshold.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800072	Warning	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
APMAC	Indicates the MAC address of an AP.
APName	Indicates the AP name.
RadioID	Indicates the radio ID of the AP.
ChannelUtil	Indicates the channel usage.
APID	Indicates the AP ID.

Impact on the System

New users cannot access the network.

Possible Causes

The channel usage exceeds the alarm threshold when users associate with the AP.

Procedure

- Step 1** Run the **uac channel-utilization threshold threshold access** *access-threshold* [**roam** *roam-threshold*] command in the radio profile view to increase the upper limit on the number of users. Then, check whether the alarm persists.
- If so, go to Step 2.
 - If not, go to Step 3.

- Step 2** Collect alarm messages, log messages, and configurations, and then contact the technical support personnel.
- Step 3** End.
- End

Related Information

None

3.3.91 ALM-3276800073 Radio signal environment deteriorates

Description

WLAN/4/RADIO_ENV_DETERIORATE:OID [OID] Radio signal environment deteriorates. (APMAC=[OPAQUE],RadioID=[INTEGER], APName=[OCTET], PER=[INTEGER]%, ConflictRate=[INTEGER]%, APID=[INTEGER], NoiseFloor=[INTEGER]dBm, Reason=[OCTET], BadChannel=[INTEGER])

The radio signal environment deteriorated.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800073	Warning	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
APMAC	Indicates the MAC address of an AP.
RadioID	Indicates the radio ID.
APName	Indicates the AP name.
PER	Indicates the packet error rate on the wireless-side interface.
ConflictRate	Indicates the collision rate of a radio.
APID	Indicates the AP ID.
NoiseFloor	Indicates the noise floor value detected in the current environment.

Name	Meaning
Reason	Indicates the noise floor generation reason.
BadChannel	Indicates the bad channel.

Impact on the System

The deterioration of the radio signal environment will increase the packet loss rate, reduce the transmission rate, or even interrupt services.

Possible Causes

The radio signal environment deteriorated.

Procedure

- Step 1** Run the **display ap neighbor** command to view the neighboring radio, and check whether there are APs using the same or neighboring radio.
- If so, run the **channel** command to reconfigure a channel or power for this radio to avoid the signal interference. Then go to [Step 2](#).
 - If not, go to [Step 3](#).
- Step 2** Check whether a radio signal environment restoration alarm is generated.
- If so, go to [Step 6](#).
 - If not, go to [Step 3](#).
- Step 3** Check whether there are devices that interfere with the radio signal or make noises.
- If so, remove these devices and then go to [Step 4](#).
 - If not, go to [Step 5](#).
- Step 4** Check whether a radio signal environment restoration alarm is generated.
- If so, go to [Step 6](#).
 - If not, go to [Step 5](#).
- Step 5** Collect the alarm information, log information, and configuration information, and then contact technical support personnel.
- Step 6** End.
- End

Related Information

None

3.3.92 ALM-3276800074 A Layer 3 service failed because of insufficient ACL resources

Description

L3MB/4/ACLRESOURCELACK: OID [OID] [OCTET]
(Slot=[OCTET],ReasonID=[INTEGER])

A Layer 3 service failed because of insufficient ACL resources.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800074	Warning	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
[OCTET]	Indicates a type of Layer 3 service. The value can be: - Failed to enable nd snooping: failed to enable the neighbor discovery (ND) snooping function. - Failed to enable ipv6: failed to enable the IPv6 function. - Failed to start nqa-rtp instance: failed to start an NQA RTP test instance.
Slot	Indicates a slot number.
ReasonID	Indicates the error code. l3aclFailed (72): failed to deliver an ACL.

Impact on the System

The Layer 3 service specified in the alarm is unavailable.

Possible Causes

ACL resources were insufficient.

Procedure

- Step 1** Run the **display acl resource [slot slot]** command to view information about ACL resources, including ACL4 and ACL6 resources.
- Step 2** Run the **display current-configuration** command to check the current configuration on the switch.
- Step 3** Check the services that occupy ACL resources based on ACL resource information and the current configuration as follows, and delete unnecessary services to release ACL resources.
- Check whether NAC, IPSG, MQC, and ACL-based simplified traffic policy services that occupy a large amount of ACL resources exist on the switch.
 - Check the services that occupy ACL resources based on fields in the ACL resource information. For example, MQC, ACL-based simplified traffic policy, SVF, MPLS, and BFD for VPLS services occupy **UDF ACL** resources. If a large amount of **UDF ACL** resources are occupied, check these services first.
- Step 4** If the fault persists, collect alarm information and configuration information, and then contact technical support personnel. You can collect diagnostic information using the **display diagnostic-information** command.

----End

Related Information

None

3.3.93 ALM-3276800075 Failed to execute the command

Description

L3MB/4/SERVICEFAILED: OID [OID] Failed to execute the command.
(Command=[OCTET],ViewName=[OCTET],ReasonID=[INTEGER],ReasonDescr=[OCTET],Slot=[OCTET])

The card fails to execute the globally delivered command due to insufficient Layer 2 user entries.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800075	Warning	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.

Name	Meaning
Command	Indicates the command name.
ViewName	Indicates the view name.
ReasonID	Indicates the error code. l2UserEntryOverload(92): insufficient Layer 2 user entries.
ReasonDescr	Indicates the alarm reason description.
Slot	Indicates the slot ID.

Impact on the System

The card fails to execute the command.

Possible Causes

The Layer 2 user entries on the card are insufficient.

Procedure

- Step 1** Check whether some MAC addresses have been configured as BPDU MAC addresses using the **bpdu mac-address** command. If so, delete unnecessary BPDU MAC addresses to release entry resources used by BPDU MAC addresses.
- Step 2** Check the VRRP configuration on the switch and delete unnecessary VRRP groups to release entry resources used by VRRP virtual MAC addresses.
- Step 3** Check the interface configuration on the switch and delete unnecessary VLANIF interfaces and Layer 3 subinterfaces to release MAC address entry resources used by these interfaces.
- Step 4** Release entry resources using the preceding steps, delete the globally delivered command that fails to be executed by the card in the system view, and then execute this command again.
- Step 5** If the preceding steps cannot resolve the entry insufficiency issue, collect alarms, logs, and configurations on the switch and contact technical support personnel.

----End

Related Information

None

3.3.94 ALM-3276800076 IPv6 cannot be enabled on the interface because of insufficient system resources

Description

L3MB/4/IPV6RESOURCELACK:OID [OID] IPv6 cannot be enabled on the interface because of insufficient resources.(vlanif=[OCTET],Slot=[OCTET])

IPv6 cannot be enabled on the interface because of insufficient system resources.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800076	Warning	processingErrorAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
vlanif	Indicates the number of the VLANIF interface.
Slot	Indicates the slot ID.

Impact on the System

The IPv6 service is unavailable in the VLANIF interface view.

Possible Causes

system resources are insufficient.

Procedure

Step 1 Adjust the usage of ACL resources.

Run the **display acl resource** command to check ACL resource information. Run the **undo ipv6 enable** command in the VLANIF interface view to disable the IPv6 function. Delete some unnecessary service configurations that occupy ACL resources to release the resources. Run the **ipv6 enable** command in the VLANIF interface view to enable the IPv6 function.

After completing the preceding operations, check whether the alarm is cleared. If yes, go to step 3; if no, go to step 2.

Step 2 Collect trap messages, log messages, and configurations, and contact technical support personnel.

Step 3 End.

----End

Related Information

None

3.3.95 ALM-3276800077 ND entries failed to be saved because of a hash conflict

Description

L3MB/3/IPV6NDFULL: OID [OID] Fail to download ND entry because of hash collision.(IPv6Address=[OCTET],VrfID=[INTEGER],Slot=[OCTET])

ND entries failed to be saved because of a hash conflict.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800077	Minor	processingErrorAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
IPv6Address	IPv6 address with the hash conflict.
VrfID	VRF ID.
Slot	Slot ID.

Impact on the System

The switch could not forward IPv6 traffic matching the ND entries.

Possible Causes

A hash conflict occurred when the ND entries were saved.

Procedure

- Step 1** Run the **display ipv6 routing-table** command to check IPv6 routes on the switch.
- Step 2** Delete unused IPv6 routes based on service requirements and the networking.
Check whether the trap is still reported.

- If the trap is still reported, go to step 3.
- If the trap is not reported, no action is required.

Step 3 Collect alarm information and configuration information, and then contact technical support personnel.

----End

Related Information

None

3.3.96 ALM-3276800078 The switch detected an anomaly when periodically checking l3-forward-entries

Description

L3MB/4/L3FWDCONFLICT:OID [OID] L3 forward entry regularly check abnormal. (Slot=[OCTET], ReasonId=[INTEGER])

The switch detected an anomaly when periodically checking l3-forward-entries.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800078	Warning	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
Slot=[OCTET]	Indicates a slot ID.
ReasonId=[INTEGER]	Indicates the error code. • nextHopTable(31) l3-forward-entries are abnormal.

Impact on the System

Layer 3 services involved in the alarm may become unavailable.

Possible Causes

By default, the switch periodically checks l3-forward-entries to ensure realtime and validity of bottom-layer forwarded data and records the check result. The check result can help locate problems of Layer 3 forwarding software resource

leak and residual Layer 3 forwarding hardware entries. When the switch detects an anomaly during l3-forward-entry check, an alarm is generated.

Procedure

This alarm is informational only, and no action is required.

Related Information

None

3.3.97 ALM-3276800079 The card failed to deliver entries during VXLAN tunnel establishment due to a hash conflict

Description

ADPVXLAN/4/VXLANTNLFAIL(t):OID [OID] Failed to add VXLAN tunnel table due to hash conflict.(Slot=[OCTET])

The device failed to deliver entries during VXLAN tunnel establishment due to a hash conflict.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800079	Warning	processingErrorAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
OCTET	Indicates the slot ID.

Impact on the System

VXLAN tunnels cannot be established, which may affect forwarding of VXLAN service traffic.

Possible Causes

The device failed to deliver entries during VXLAN tunnel establishment due to a hash conflict.

Procedure

- Step 1** Configure VXLAN tunnels and deliver entries again and then check whether the alarm is cleared.
- If so, go to step 3.
 - If not, go to step 2.
- Step 2** Contact technical support personnel.
- Step 3** End.
- End

3.3.98 ALM-3276800080 The VXLAN-incapable card failed to decapsulate received VXLAN packets

Description

ADPVXLAN/4/NOSUPPENCAPDECAPPKTS(t):OID [OID] The slot does not support to encapsulate and decapsulate VXLAN packets.
(Slot=[OCTET1],Vni=[INTEGER],SourceIP=[OCTET2],PeerIP=[OCTET3])

The VXLAN-incapable device failed to decapsulate received VXLAN packets.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800080	Warning	processingErrorAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
OCTET1	Indicates the slot ID.
INTEGER	Indicates the VNI ID of VXLAN packets.
OCTET2	Indicates the source VTEP IP address of VXLAN packets.
OCTET3	Indicates the remote VTEP IP address of VXLAN packets.

Impact on the System

VXLAN service traffic may fail to be forwarded.

Possible Causes

The device does not support VXLAN packet decapsulation.

Procedure

- Step 1** Run the **display arp** command to locate the interface receiving VXLAN packets based on the source VTEP IP address in the alarm, and check whether the device where the interface resides supports VXLAN packet decapsulation.
- If so, go to step 3.
 - If not, go to step 2.
- Step 2** Replace the interface with the one supporting VXLAN packet decapsulation, and then check whether the alarm is cleared.
- If so, go to step 4.
 - If not, go to step 3.
- Step 3** Contact technical support personnel.
- Step 4** End.
- End

3.3.99 ALM-3276800081 MAC address learning reached the limit

Description

L2IFPPI/4/MAC_LIMIT_ALARM: OID [OID] MAC address learning reached the limit. (L2IfNum=[INTEGER], MacLimitVlanId=[INTEGER], MacLimitVsiName=[OCTET], L2PortNum=[INTEGER], BaseTrapSeverity=[INTEGER], BaseTrapProbableCause=[INTEGER], BaseTrapEventType=[INTEGER], MacDynAddressLearnNum=[INTEGER], MacLimitMaxMac=[INTEGER], L2IfPortName=[OCTET])

The number of MAC addresses learned by the interface, VLAN, or VSI reached the upper limit.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800081	Warning	other(1)

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.

Name	Meaning
L2IfNum	Indicates the interface index.
MacLimitVlanId	Indicates the VLAN ID.
MacLimitVsiName	Indicates the VSI name.
L2PortNum	Indicates the port index.
BaseTrapSeverity	Indicates the alarm severity.
BaseTrapProbableCause	Indicates the alarm cause.
BaseTrapEventType	Indicates the alarm type.
MacDynAddressLearnNum	Indicates the number of learned MAC addresses.
MacLimitMaxMac	Indicates the maximum number of MAC addresses to be learned.
L2IfPortName	Indicates the interface name.

Impact on the System

No more MAC addresses can be learned.

Possible Causes

The number of MAC addresses learned by the interface, VLAN, or VSI reached the upper limit.

Procedure

Step 1 Check whether the alarm is generated on an interface, in a VLAN, or in a VSI.

Perform one of the following operations according to networking requirements and go to step 2:

- Increase the upper limit on the number of MAC addresses to be learned.
- Delete unnecessary MAC addresses.
- Ignore the alarm.

Step 2 End.

----End

Related Information

None

3.3.100 ALM-3276800082 MAC address information

Description

L2IFPPI/5/MACCHANGE_TRAPINFO: OID [OID] MAC address information:
[OCTET].

The MAC address changes.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800082	Indeterminate	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.

Name	Meaning
OCTET	Indicates TypeIfindexVlaninvalidVlanid-Mac-address. The fields are described as follows: • Type: reason why MAC addresses change. 01 indicates MAC address learning; 02 indicates MAC address aging. • Ifindex: index of the interface sending the MAC address change alarm. • Vlaninvalid: VLAN tag. The value 1 indicates that the MAC address is learned in VLAN. • Vlanid: VLAN ID. • Mac-address: MAC address. A sample of the alarm message: L2IFPPI/5/MACCHANGE_TRAPINFO: OID 1.3.6.1.4.1.2011.5.25.315.3.1 Mac address information:0200000006103e8000011105ee. The fields in the alarm are described as follows: • 02: MAC address aging. • 00000006: interface index. • 1: MAC address is learned in VLAN. • 03e8: The decimal notation of this value is 1000. That is, this field indicates VLAN 1000. • 0000111105ee: MAC address that is aged out.

Impact on the System

None

Possible Causes

The device learns the MAC address or the MAC address is aged.

Procedure

This alarm is informational only, and no action is required.

Related Information

None

3.3.101 ALM-3276800083 The MAC Address usage exceeds the threshold

Description

L2IFPPI/4/MACEXCDALARM:OID [OID] The MAC Address usage exceeds the threshold. (MacUsageIndex=[INTEGER1], BaseTrapType=[INTEGER2], TrapSeverity=[INTEGER3], BaseTrapCause=[INTEGER4], MacUsage=[INTEGER5], MacUsageThreshold=[INTEGER6], PhysicalName=[OCTET])

The MAC address usage exceeds the upper alarm threshold.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800083	Warning	other(1)

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
INTEGER1	Indicates the index of the MAC address usage.
INTEGER2	Indicates the sending type.
INTEGER3	Indicates the sending severity.
INTEGER4	Indicates the sending cause.
INTEGER5	Indicates the MAC address usage.
INTEGER6	Indicates the alarm threshold for the MAC address usage.
OCTET	Indicates the interface name.

Impact on the System

MAC addresses on the device may fail to be learned. As a result, Layer 2 unicast packets are broadcast.

Possible Causes

The MAC address usage exceeds the upper alarm threshold.

Procedure

Step 1 Check whether the threshold of the MAC address usage is too low. By default, the lower threshold is 70% and the upper threshold is 80%. Users can specify the threshold range according to service requirements.

- If so, go to step 2.
- If not, go to step 3.

Step 2 Run the **mac-address threshold-alarm upper-limit upper-limit-value lower-limit lower-limit-value** command in the system view to reset the alarm thresholds. Check whether the alarm is cleared.

- If so, go to step 5.
- If not, go to step 3.

Step 3 Use either of the following methods:

- Migrate services to other idle devices or load balance services to different devices.
- Run the **assign resource-mode enhanced-mac slot slot-id** command in the system view to configure the extended MAC entry resource mode.

NOTE

After the extended MAC entry resource mode is configured, you must restart the device to make the configuration take effect.

For details about models that support the extended MAC entry resource mode, see **assign resource-mode**.

When the **enhanced-mac** mode is configured to increase the specifications of MAC address entries, specifications of other entries are affected. For details about the specifications of each entry in the **enhanced-mac** mode, see **assign resource-mode**.

After the operation, check whether the alarm persists.

- If so, go to step 4.
- If not, go to step 5.

Step 4 Collect alarm, log, and configuration information, and contact technical support personnel.

Step 5 End.

----End

Related Information

None

3.3.102 ALM-3276800084 The MAC Address usage falls below the threshold

Description

L2IFPPI/4/MACEXCDALARM: OID [OID] The MAC Address usage falls below the threshold. (PhysicalIndex=[INTEGER1], BaseTrapType=[INTEGER2], TrapSeverity=[INTEGER3], BaseTrapCause=[INTEGER4], PhysicalName=[OCTET])

The MAC address usage is lower than the lower alarm threshold.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800084	Warning	other(1)

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
INTEGER1	Indicates the instance ID.
INTEGER2	Indicates the sending type.
INTEGER3	Indicates the sending severity.
INTEGER4	Indicates the sending cause.
OCTET	Indicates the interface name.

Impact on the System

None

Possible Causes

The MAC address usage is lower than the lower alarm threshold.

Procedure

This trap message is informational only, and no action is required.

Related Information

None

3.3.103 ALM-3276800085 The LPU is powered off

Description

L2IFPPI/4/BOARDPOWEROFF: OID [OID] The LPU is powered off. This LPU only supports the trunks with index 127 or smaller than 127. Delete the trunks with index larger than 127 and power on the LPU. (Index=[INTEGER1], EntityPhysicalIndex=[INTEGER2], PhysicalName="[OCTET]", EntityTrapEntType=[INTEGER3], EntityTrapFaultID=[INTEGER4])

The card was powered off. The card supports only the Eth-Trunk with the index less than or equal to 127. Delete the Eth-Trunk with the index larger than 127, and power on the card.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800085	Warning	environmentalAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
OCTET	Indicates the entity name.
INTEGER1	Indicates the instance index.
INTEGER2	Indicates the index of the physical entity.
INTEGER3	Indicates the entity type.
INTEGER4	Indicates the error code.

Impact on the System

The card cannot be registered.

Possible Causes

The causes are as follows:

Only some cards support Eth-Trunk specification extension. If Eth-Trunk specification extension is configured and there is an Eth-Trunk with the index larger than 127, when you install the card that does not support Eth-Trunk specification (low-specification card), the low-specification card cannot be registered.

Procedure

Step 1 Use either of the following methods:

- Remove the low-specification card. For details about the supported cards, see the **assign trunk** command.
- If the low-specification card must be used, delete the Eth-Trunk with the index larger than 127. For details about the mapping between Eth-Trunk indexes and IDs, see the **display trunk index-map** command.

Step 2 If the alarm is not cleared, contact technical support personnel.

Step 3 End.

----End

Related Information

None

3.3.104 ALM-3276800086 The rapid-change of input broadcast exceeded the threshold

Description

IFPDT/4/PORT_INBRDCAST: OID [OID] The rapid-change of input broadcast exceeded the threshold. (IfIndex=[INTEGER], InterfaceName=[STRING], InputBroadcastChangeThreshold=[INTEGER]pps, CurrentInputBroadcastRate=[COUNTER64]pps, BaseInputBroadcastRate=[COUNTER64]pps)

The difference (increase or decrease) in the broadcast traffic volume change in the inbound direction of interfaces exceeded the threshold.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800086	Warning	Quality of service alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
IfIndex	Indicates the interface index.
InterfaceName	Indicates the interface name.

Name	Meaning
InputBroadcastChangeThreshold	Indicates the threshold of the broadcast packet rate change in the inbound direction of interfaces.
CurrentInputBroadcastRate	Indicates the broadcast packet rate in the inbound direction of interfaces in the current traffic statistics collection interval.
BaseInputBroadcastRate	Indicates the base broadcast packet rate in the inbound direction of interfaces.

Impact on the System

- If the **CurrentInputBroadcastRate** value is greater than or equal to the sum of the **BaseInputBroadcastRate** and **InputBroadcastChangeThreshold** values, packet loss may occur on the switch.
- If the **CurrentInputBroadcastRate** value is less than or equal to the **BaseInputBroadcastRate** value minus the **InputBroadcastChangeThreshold** value, there is no impact.

Possible Causes

- If the **CurrentInputBroadcastRate** value is greater than or equal to the sum of the **BaseInputBroadcastRate** and **InputBroadcastChangeThreshold** values, a loop might occur on the network and caused a broadcast storm.
- If the **CurrentInputBroadcastRate** value is less than or equal to the **BaseInputBroadcastRate** value minus the **InputBroadcastChangeThreshold** value, the broadcast traffic volume in the inbound direction of interfaces restored.

The sudden traffic volume increase trap and sudden traffic volume change clear trap are timed respectively. After a sudden traffic volume increase trap or sudden traffic volume change clear trap is generated, the switch will not generate the trap again within 10 minutes.

Procedure

- If the **CurrentInputBroadcastRate** value is greater than or equal to the sum of the **BaseInputBroadcastRate** and **InputBroadcastChangeThreshold** values, check whether the broadcast traffic volume increase is normal. If not, check whether a loop exists on the link.
- If the **CurrentInputBroadcastRate** value is less than or equal to the **BaseInputBroadcastRate** value minus the **InputBroadcastChangeThreshold** value, this trap is informational only, and no action is required.

3.3.105 ALM-3276800087 The input rate change ratio exceeded the threshold

Description

IFPDT/4/PORT_INRATECHG: OID [OID] The input rate change ratio exceeded the threshold. (IfIndex=[INTEGER], InterfaceName=[STRING], ThresholdPercent=[INTEGER]%, CurrentStatisticalPeriodRate=[COUNTER64], LastStatisticalPeriodRate=[COUNTER64])

The sudden traffic volume change percentage in the inbound direction of interfaces exceeded the trap threshold.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800087	Warning	Quality of service alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
IfIndex	Indicates the interface index.
InterfaceName	Indicates the interface name.
ThresholdPercent	Indicates the detection threshold of sudden traffic volume changes.
CurrentStatisticalPeriodRate	Interface rate in the current traffic statistics collection interval.
LastStatisticalPeriodRate	Interface rate in the previous traffic statistics collection interval.

Impact on the System

Packet loss may occur on interfaces.

Possible Causes

The sudden traffic volume change percentage in the inbound direction of interfaces exceeded the trap threshold.

Procedure

- Step 1** Run the **display this interface** command to view the **Input bandwidth utilization** field, and check whether the sudden traffic in the inbound direction of interfaces is normal.
- If so, no action is required.
 - If not, check whether a loop exists on the link.
- Step 2** Collect log information, and contact technical support personnel.
- End

3.3.106 ALM-3276800088 The Output Rate Change Ratio Exceeded the Threshold

Description

IFPDT/4/PORT_OUTRATECHG: OID [OID] The output rate change ratio exceeded the threshold. (IfIndex=[INTEGER], InterfaceName=[STRING], ThresholdPercent=[INTEGER]%, CurrentStatisticalPeriodRate=[COUNTER64], LastStatisticalPeriodRate=[COUNTER64])

The sudden traffic volume change percentage in the outbound direction of interfaces exceeded the trap threshold.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800088	Warning	Quality of service alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
IfIndex	Indicates the interface index.
InterfaceName	Indicates the interface name.
ThresholdPercent	Indicates the detection threshold of sudden traffic volume changes.
CurrentStatisticalPeriodRate	Rate of bytes on the interface in the current traffic statistics collection interval.
LastStatisticalPeriodRate	Rate of bytes on the interface in the previous traffic statistics collection interval.

Impact on the System

Packet loss may occur on interfaces.

Possible Causes

The sudden traffic volume change percentage in the outbound direction of interfaces exceeded the trap threshold.

Procedure

- Step 1** Run the **display this interface** command to view the **Output bandwidth utilization** field, and check whether the sudden traffic in the inbound direction of interfaces is normal.
- If so, no action is required.
 - If not, check whether a loop exists on the link.
- Step 2** Collect log information, and contact technical support personnel.
- End

3.3.107 ALM-3276800089 IP Address-based Load Balancing on an Eth-Trunk Interface Fails to Take Effect for VXLAN Packets When It Functions as an Outbound Interface of VXLAN Packets

Description

IFPDT/4/VXLANHASHNOTSUPPORT:OID [OID] The Eth-Trunk can not function normally as an outbound interface for vxlan packets when IP address-based load balancing is configured. (InterfaceIndex=[INTEGER], InterfaceName=[STRING])

When an Eth-Trunk interface functions as an outbound interface of VXLAN packets, IP address-based load balancing configured on the Eth-Trunk interface does not take effect for VXLAN packets.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800089	Warning	Communication alarm

Parameters

Name	Meaning
OID	MIB object ID of the alarm.

Name	Meaning
InterfaceIndex	Interface index.
InterfaceName	Interface name.

Impact on the System

When an Eth-Trunk interface functions as an outbound interface of VXLAN packets, IP address-based load balancing configured on the Eth-Trunk interface does not take effect for VXLAN packets.

Possible Causes

When the Eth-Trunk interface functions as an outbound interface of VXLAN packets, it has IP address-based load balancing in common mode configured.

Procedure

- Clear the alarm through iMaster NCE-Campus.
 - Clear the alarm through the CLI.
 - i. Log in to iMaster NCE-Campus as a tenant administrator and choose **Plan > Provision > Configuration > Site Configuration** from the main menu. Choose **Site > CLI** on the **Site Configuration** tab page.
 - ii. Run the **load-balance {dst-mac}** command on the Eth-Trunk interface to configure MAC address-based load balancing. Check whether the alarm is cleared.
 - If so, go to Step 4.
 - If not, go to Step 3.
 - iii. Collect alarm, log, and configuration information, and contact technical support personnel.
 - iv. End.
 - Clear the alarm through the controller web UI.
 - i. Log in to iMaster NCE-Campus as a tenant administrator and choose **Plan > Provision > Configuration > Site Configuration** from the main menu. On the **Site Configuration** tab page, choose **Switch > Interface**.
 - ii. On the **Select Interface** page, select the device and Eth-Trunk interface to be configured.
 - iii. Expand **Advanced** and set **Load balancing** to **Destination MAC Address**.
 - iv. End.
- Clear the alarm through the device CLI.
 - a. Run the **load-balance {dst-mac}** command on the Eth-Trunk interface to configure MAC address-based load balancing. Check whether the alarm is cleared.

- i. If so, go to Step 3.
 - ii. If not, go to Step 2.
- b. Collect alarm, log, and configuration information, and contact technical support personnel.
- c. End.

3.3.108 ALM-3276800090 Channel of radio is changed

Description

WLAN/4/RADIO_CHANNEL_CHANGE:OID [OID] Channel of radio is changed.
(APMAC=[OPAQUE], RadioID=[INTEGER], APName=[OCTET], Channel1=[OCTET], Channel2=[OCTET], CauseId=[INTEGER], CauseStr=[OCTET], PreChannel1=[OCTET], PreChannel2=[OCTET], APID=[INTEGER], NewChannelHasRadarChannel=[OCTET])

The AP channel was changed.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800090	Warning	environmentalAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
APMAC	Indicates the MAC address of an AP.
RadioID	Indicates the radio ID.
APName	Indicates the AP name.
Channel1	Indicates the actual working channel of the AP.
Channel2	Indicates the actual second working channel of the AP.

Name	Meaning
CauseId	Indicates the channel change reason. - unknown(1) - The channel was changed due to an unknown reason. - dfs(2) - The channel was changed due to Dynamic Frequency Selection (DFS). - wds(3) - The channel was changed due to WDS network establishment. - config(4) - The channel was changed due to manual configurations. - calibrate(5) - The channel was changed due to radio calibration. - thirdGPP(6) - The channel was changed due to 3GPP base station notification.
CauseStr	Indicates a character string describing channel change reasons.
PreChannel1	Indicates the channel before change. NOTE When an AP goes online on an AC for the first time, the channel of the AP before change is not saved on the AC. Therefore, when a channel change alarm is generated for the first time, the original channel of the AP is displayed as - in the alarm.
PreChannel2	Indicates the second channel before the channel is changed.
APID	Indicates the AP ID.
NewChannelHasRadarChannel	Indicates whether radar channels exist among the changed channels.

Impact on the System

The working channel of the AP was changed, which may affect the other APs.

Possible Causes

Cause 1: The radio was calibrated.

Cause 2: Users changed the channel.

Cause 3: Radar signals conflicted.

Cause 4: The channel changed in WDS mode.

Cause 5: The channel changed in Mesh mode.

Procedure

This alarm is informational only, and no action is required.

Related Information

None

3.3.109 ALM-3276800091 User attack occurred

Description

SECE/4/STRACKUSER: OID [OID] An attack occurred. (Interface=[OCTET], SourceMAC=[OCTET], InnerVlan=[INTEGER], OuterVlan=[INTEGER], EndTime=[OCTET], TotalPackets=[INTEGER])

The system detects an attack.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800091	Warning	securityServiceOrMechanismViolation(10)

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
Interface	Indicates the access interface of the attacker.
SourceMAC	Indicates the Source MAC address of packets sent from the attacker.
InnerVlan	Indicates the inner VLAN ID of packets sent from the attacker.
OuterVlan	Indicates the outer VLAN ID of packets sent from the attacker.
EndTime	Indicates the end time of the attack.
TotalPackets	Indicates the number of packets received from the attacker.

Impact on the System

The CPU is busy processing attack packets. As a result, normal service packets cannot be processed in time or even discarded.

Possible Causes

The rate of packets with the specified MAC address and VLAN ID sent to the CPU exceeds the alarm threshold specified by the **auto-defend threshold** command. By default, the alarm threshold is 60 pps.

Procedure

- Step 1** Run the **display auto-defend attack-source detail** command to check the possible attack source and check whether the system is normal according to the protocol type and packet increase rate.
- Step 2** If the user initiates the attack, you can configure attack source tracing and set the action taken on attack packets to deny, or configure a traffic policy to discard attack packets.
- Step 3** If the fault cause is unknown, collect device configurations, alarms, and logs, and then contact technical support personnel.
- Step 4** End.

----End

Related Information

None

3.3.110 ALM-3276800092 Port attack occurred

Description

SECE/4/STRACKPORT: OID [OID] An attack occurred. (Interface=[OCTET], InnerVlan=[INTEGER], OuterVlan=[INTEGER], EndTime=[OCTET], TotalPackets=[INTEGER])

The system detects an attack on an interface.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800092	Warning	securityServiceOrMechanismViolation(10)

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
Interface	Indicates the access interface of the attacker.
InnerVlan	Indicates the inner VLAN ID of the attacker.
OuterVlan	Indicates the outer VLAN ID of packets sent from the attacker.
EndTime	Indicates the end time of the attack.
TotalPackets	Indicates the number of packets received from the attacker.

Impact on the System

The CPU is busy processing attack packets. As a result, normal service packets cannot be processed in time or even discarded.

Possible Causes

The rate of packets with the specified interface and VLAN ID sent to the CPU exceeds the alarm threshold specified by the **auto-defend threshold** command. By default, the alarm threshold is 60 pps.

Procedure

- Step 1** Run the **display auto-defend attack-source detail** command to check the possible attack source on an interface and check whether the interface is normal according to the packet increase rate in entries.
 - Step 2** If an attack is initiated by a user and the user is the only one connected to the interface, you can shut down the interface and check whether the interface is normal.
 - Step 3** If the interface is connected to multiple users and some users initiate attacks, you can configure attack source tracing and set the action taken on attack packets to deny, or configure a traffic policy to discard attack packets.
 - Step 4** If only entries exist on the interface or entries cannot be determined, collect device configurations, alarms, and logs, and then contact technical support personnel.
 - Step 5** End.
- End

Related Information

None

3.3.111 ALM-3276800094 StormCtrl occurred

Description

SECE/4/TRAP:STORMCONTROL: OID [OID],StormControlAlarm.
(IfIndex=[INTEGER], BroadcastMinRate=[INTEGER], BroadcastMaxRate=[INTEGER], MulticastMinRate=[INTEGER], MulticastMaxRate=[INTEGER], Action=[INTEGER], Interval=[INTEGER], Status=[INTEGER], UnicastMinRate=[INTEGER], UnicastMaxRate=[INTEGER], BroadcastMode=[INTEGER], MulticastMode=[INTEGER], UnicastMode=[INTEGER])

The interface status changes.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800094	Warning	securityServiceOrMechanismViolation(10)

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
IfIndex	Indicates the interface index.
BroadcastMinRate	Indicates the minimum rate of broadcast packets.
BroadcastMaxRate	Indicates the maximum rate of broadcast packets.
MulticastMinRate	Indicates the minimum rate of multicast packets.
MulticastMaxRate	Indicates the maximum rate of multicast packets.
Action	Indicates the storm control action.
Interval	Indicates the interval for detecting storms.

Name	Meaning
Status	Indicates the interface status, including: • blocked: When the rate of receiving packets is greater than the value of MaxRate and the storm control action is block, the status of the interface is block. • normal: Packets are normally forwarded. • error-down: When the rate of receiving packets is greater than the value of MaxRate and the storm control action is error-down, the status of the interface is error-down.
UnicastMinRate	Indicates the minimum rate of unknown unicast packets.
UnicastMaxRate	Indicates the maximum rate of unknown unicast packets.
BroadcastMode	Indicates the storm control mode of broadcast packets.
MulticastMode	Indicates the storm control mode of multicast packets.
UnicastMode	Indicates the storm control mode of unknown unicast packets.

Impact on the System

Storms may occur if the threshold is exceeded. Services are not affected.

Possible Causes

The interface traffic volume is greater than the upper threshold or smaller than the lower threshold.

Procedure

- Step 1** Run the **display storm-control interface** command to check the storm control configuration on the interface.
- Step 2** If the interface status is **error-down**, check whether the interface can be enabled according to the application scenario.
- If yes, run the **shutdown** and **undo shutdown** command manually. Then go to step 4.

- If not, go to step 3.

Step 3 Collect the device configurations, alarms, and logs, and then contact technical support personnel.

Step 4 End.

----End

Related Information

None

3.3.112 ALM-3276800095 AP work mode is changed notify

Description

WLAN/4/AP_WORK_MODE_CHANGE: OID [OID] AP work mode is changed notify. (APMAC=[OPAQUE], RadioID=[INTEGER], APName=[OCTET], Mode=[INTEGER], PreMode=[INTEGER], APID=[INTEGER], ModeDesc=[STRING], PreModeDesc=[STRING])

The wireless monitoring mode of an AP was changed.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800095	Warning	Equipment alarm

Parameters

Name	Meaning
oid	Indicates the MIB object ID of the alarm.
APMAC	Indicates the MAC address of an AP.
APName	Indicates the AP name.
RadioID	Indicates the radio ID.
Mode	Indicates the current wireless monitoring mode of an AP. • 0: initial status after the AP goes online • 1: normal mode • 2: monitor mode • 3: hybrid mode

Name	Meaning
PreMode	Indicates the previous wireless monitoring mode of an AP. • 0: initial status after the AP goes online • 1: normal mode • 2: monitor mode • 3: hybrid mode
APID	Indicates the AP ID.
ModeDesc	Indicates the description of the current work mode of an AP.
PreModeDesc	Indicates the description of the previous work mode of an AP.

Impact on the System

None

Possible Causes

The work mode of the AP was changed.

Procedure

This alarm is informational only, and no action is required.

Related Information

None

3.3.113 ALM-3276800096 Gateway conflict

Description

SECE/4/GATEWAY_CONFLICT: OID [OID] Gateway conflict.
(SourceInterface=[OCTET], SourceIP=[OCTET], SourceMAC=[OCTET],
OuterVlan=[INTEGER], InnerVlan=[INTEGER])

The system detects attack packets whose source IP addresses are the same as the gateway IP address.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800096	Warning	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
SourceInterface	Indicates the source interface of packets.
SourceIP	Indicates the source IP address of packets.
SourceMAC	Indicates the source MAC address of packets.
OuterVlan	Indicates the outer VLAN ID of packets.
InnerVlan	Indicates the inner VLAN ID of packets.

Impact on the System

If this alarm is generated, the user gateway information may be modified by an attacker. As a result, the user is attacked and user services are interrupted.

Possible Causes

The device is attacked by packets whose source IP address is the same as the gateway IP address.

Procedure

- Step 1** Find the interface where the gateway conflict occurs according to the value of **SourceInterface**.
- Step 2** Lock the user who sends gateway conflict packets according to the values of **SourceMAC** and **OuterVlan**.
- Step 3** Check whether the allocated address of the user conflicts with the gateway address. If the address conflicts, allocate an address to the user again. If the address does not conflict, the user may be the attacker. In this case, you can take such measures as disconnecting the user.

----End

Related Information

None

3.3.114 ALM-3276800097 Invalid ARP packet

Description

SECE/4/ARP_PACKET_CHECK: OID [OID] Invalid packet. (SourceInterface=[OCTET], SourceIP=[OCTET], SourceMAC=[OCTET], OuterVlan=[INTEGER], InnerVlan=[INTEGER])

The system detects invalid ARP packets.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800097	Warning	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
SourceInterface	Indicates the source interface of packets.
SourceIP	Indicates the source IP address of packets.
SourceMAC	Indicates the source MAC address of packets.
OuterVlan	Indicates the outer VLAN ID of packets.
InnerVlan	Indicates the inner VLAN ID of packets.

Impact on the System

If this alarm is generated, the device may be attacked. If the attack traffic volume is heavy, the device is busy processing attack packets. As a result, services of authorized users are interrupted.

Possible Causes

The device receives invalid ARP packets.

Procedure

- Step 1** Find the interface where the gateway conflict occurs according to the value of **SourceInterface**.

- Step 2** Lock the user who sends gateway conflict packets according to the values of **SourceMAC** and **PVLAN**.
- Step 3** Check whether the allocated address of the user conflicts with the gateway address. If the address conflicts, allocate an address to the user again. If the address does not conflict, the user may be the attacker. In this case, you can take such measures as disconnecting the user.
- End

Related Information

None

3.3.115 ALM-3276800098 Dai drop alarm

Description

SECE/4/DAI_DROP_ALARM: OID [oid] The packet number dropped by DAI reaches [INTEGER], exceed the alarm threshold [INTEGER], Interface [OCTET].

The number of packets discarded by Dynamic ARP Inspection (DAI) on an interface exceeds the alarm threshold.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800098	Warning	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
INTEGER1	Indicates the number of discarded packets.
INTEGER2	Indicates the alarm threshold.
Interface	Indicates the VLAN, source MAC address, and source IP address of packets

Impact on the System

If this alarm is generated, the device may be attacked. If the attack traffic volume is heavy, the device is busy processing attack packets. As a result, services of authorized users are interrupted.

Possible Causes

The number of packets discarded by DAI exceeds the alarm threshold. By default, the alarm threshold for ARP packets discarded by DAI is 100 packets.

Procedure

- If user services are not affected, the alarm does not need to be handled.
- If user services are interrupted, perform the following operations:
 - a. Run the **display dhcp static user-bind** { { **interface** *interface-type interface-number* | **ip-address** *ip-address* | **mac-address** *mac-address* | **vlan** *vlan-id* } * | **all** } [**verbose**] or **display dhcpv6 static user-bind** { { **interface** *interface-type interface-number* | **ipv6-address** { *ipv6-address* | **all** } | **mac-address** *mac-address* | **vlan** *vlan-id* } * | **all** } [**verbose**] command to check the static binding entries.
 - b. Find out the interface and user host that initiate the attack. Check whether the host is attacked. If not, the host belongs to the attacker. Take measures to defend against the attack, for example, disconnect the attacker's host.
 - c. Collect alarm and configuration information, and contact technical support personnel.

Related Information

None

3.3.116 ALM-3276800100 Global arp-miss exceed the speed-limit

Description

SECE/4/ARPMISS_SIP_SPEEDLIMIT_ALARM: OID [OID] The arp-miss packet speed with source ip [OCTET] exceed the speed-limit value configed [INTEGER].

The rate of ARP Miss messages with the specified source IP address exceeds the configured alarm threshold.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800100	Warning	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.

Name	Meaning
OCTET	Indicates the source IP address of packets.
INTEGER	Indicates the alarm threshold.

Impact on the System

If the alarm is generated, the user traffic volume exceeds the threshold. The device discards excess traffic. As a result, user traffic may be interrupted intermittently.

Possible Causes

If a host sends a large number of IP packets with unresolvable destination IP addresses to attack a device (the device has a route to the destination IP address of a packet but has no ARP entry matching the next hop of the route), the device generates a large number of ARP Miss messages. When the rate of ARP Miss messages with the specified source IP address exceeds the alarm threshold, the device generates the alarm.

Procedure

- Step 1** Run the **reset cpu-defend statistics** command to clear statistics on the ARP Miss messages sent to the CPU.
- Step 2** Wait for 1 minute, and run the **display cpu-defend statistics all** command to check the number of ARP Miss messages sent to the CPU within 1 minute. Check whether a large number of packets are discarded:
- If so, locate the attack source according to the IP address in the alarm information and check whether the attack source is attacked by viruses.
 - If so, you are advised to remove viruses from the user host. You can also add the address of the user to the blacklist or configure a blackhole MAC address entry to discard ARP request packets sent by the attacker.
 - If not, go to step 3.
 - If not, verify that the network is secure and use either of the following methods to prevent generation of this alarm:
 - Run the **arp-miss speed-limit source-ip [ip-address] maximum 0** command to disable the rate limit on ARP Miss messages based on source IP addresses.
 - If ip-address is not specified, ARP Miss message rate limiting is disabled for all source IP addresses. If a large number of ARP Miss messages are generated for a certain source IP address, the CPU usage may be excessively high.
 - If ip-address is specified, ARP Miss message rate limiting is disabled for this source IP address. If a large number of ARP Miss messages are generated for the source IP address, the CPU usage may be excessively high.
 - Run the **info-center source SECE channel 4 log state off** command to disable the device from sending SECE alarm information.

- Step 3** Run the **display arp anti-attack configuration arpmiss-speed-limit** command to check the configuration of source-based ARP-Miss suppression.
- Step 4** Run the **arp-miss speed-limit source-ip [ip-address] maximum** maximum command to modify the maximum rate of ARP Miss messages based on the site requirements.
- Step 5** If the alarm is frequently generated, collect alarm information and contact technical support personnel.
- End

3.3.117 ALM-3276800101 IPSG drop

Description

SECE/4/IPSG_DROP_ALARM: OID [OID] The packet number dropped by IPSG reaches [INTEGER1], exceed the alarm threshold [INTEGER2], interface [OCTET].

The number of packets discarded by IPSG exceeded the alarm threshold.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800101	Warning	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
INTEGER1	Indicates the number of discarded packets.
INTEGER2	Indicates the alarm threshold.
OCTET	Indicates the source interface, VLAN, source MAC address, and source IP address of packets.

Impact on the System

If this alarm is generated, the device may be attacked. If the attack traffic volume is heavy, the device is busy processing attack packets. As a result, services of authorized users are interrupted.

Possible Causes

The number of packets discarded by IPSG exceeded the alarm threshold. This threshold can be configured using the **ip source check user-bind alarm threshold** command. The default alarm threshold is 100.

Procedure

- Step 1** Find the interface where attacks occur according to **Interface** in the alarm message.
- Step 2** Check whether users who are not in the DHCP snooping binding table range are connected.
- Step 3** If new users are connected, run related DHCP snooping commands to generate the DHCP snooping binding table.

----End

Related Information

None

3.3.118 ALM-3276800102 Global ICMP exceed the speed-limit

Description

SECE/4/ICMP_GLOBAL_SPEEDLIMIT_ALARM: OID [OID]. Global icmp packet speed exceed the speed-limit value configured [INTEGER].

The rate of ICMP packets exceeds the alarm threshold.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800102	Warning	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
INTEGER	Indicates the alarm threshold.

Impact on the System

If the alarm is generated, it indicates that the user traffic volume exceeds the threshold. The excess traffic is discarded by the device. As a result, user traffic may be interrupted intermittently.

Possible Causes

The global ICMP packet rate exceeds the alarm threshold.

Procedure

- If user services are not affected, the alarm does not need to be handled.
- If the user services are intermittently disconnected, run the **icmp rate-limit total threshold** threshold-value command in the system view to adjust the global ICMP rate limit. Increasing the rate limit may affect CPU usage. You are advised to contact technical support personnel.

Related Information

None

3.3.119 ALM-3276800103 Interface ICMP exceed the speed-limit

Description

SECE/4/ICMP_IF_SPEEDLIMIT_ALARM: OID [OID] Interface icmp packet speed exceed the speed-limit value configed [INTEGER], Interface [OCTET].

The rate of ICMP packets on an interface exceeds the alarm threshold.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800103	Warning	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
INTEGER1	Indicates the alarm threshold.
Interface	Indicates the source interface of packets.

Impact on the System

If the alarm is generated, it indicates that the user traffic volume exceeds the threshold. The excess traffic is discarded by the device. As a result, user traffic may be interrupted intermittently.

Possible Causes

The rate of ICMP packets on an interface exceeds the alarm threshold.

Procedure

- If user services are not affected, the alarm does not need to be handled.
- If the user services are intermittently disconnected, run the **icmp rate-limit interface** interface-type interface-number [**to** interface-number] **threshold** threshold-value command in the system view to adjust the ICMP rate limit on an interface. Increasing the rate limit may affect CPU usage. You are advised to contact technical support personnel.

Related Information

None

3.3.120 ALM-3276800104 The System Detected an Attack Source and Dropped Packets Sent from the Attack Source

Description

SECE/4/STRACK_DENY: OID [OID] Some packets are dropped because an attack is detected. (Interface=[OCTET], SourceMAC=[OCTET], SourceIP=[OCTET], InnerVlan=[INTEGER], OuterVlan=[INTEGER])

The system detected an attack source and dropped packets sent from the attack source.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800104	Warning	securityServiceOrMechanismViolation(10)

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
Interface	Indicates the access interface of the attacker.

Name	Meaning
SourceMAC	Indicates the Source MAC address of packets sent from the attacker.
SourceIP	Indicates the Source IP address of packets sent from the attacker.
InnerVlan	Indicates the inner VLAN ID of packets sent from the attacker.
OuterVlan	Indicates the outer VLAN ID of packets sent from the attacker.

Impact on the System

The device detected an attack to the CPU and dropped packets sent from the attack source to the CPU.

Possible Causes

A user sent a large number of packets to the user, and the number of packets exceeded the threshold for identifying an attack.

Procedure

- Step 1

Run the **display auto-defend attack-source detail** command to check the detected attack source and check whether it is an authorized user.
- Step 2

If the detected attack source is an unauthorized user, you do not need to take any actions because the attack packets have been dropped by the device. Go to Step 6.
- Step 3

If the detected attack source is an authorized user, add the user to the whitelist to exclude the user from attack source tracing.
- Step 4

If multiple attack sources are detected and all of them are authorized users, the attack source tracing threshold is too low. (The default value is 128 pps). Run the **auto-defend threshold** *threshold* command to increase the threshold. Go to Step 6.
- Step 5

If the alarm persists, collect the configuration, alarms, and logs of the device and contact technical support personnel.
- Step 6

End.
- End

Related Information

None

3.3.121 ALM-3276800105 An Attack Source Is Detected and the Source Interface of Attack Packets to Error-Down State

Description

SECE/4/STRACK_ERROR_DOWN: OID [OID] Interface's status is changed to error-down because an attack is detected, Interface [OCTET].

The system detected an attack source and set the source interface of the attack packets to error-down state.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800105	Warning	securityServiceOrMechanismViolation(10)

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
Interface	Indicates the access interface of the attacker.

Impact on the System

The interface in error-down state cannot work.

Possible Causes

The device received a large number of packets from the interface, and the rate of received packets exceeded the alarm threshold specified by the **auto-defend threshold** command to identify an attack. Therefore, the device identified the interface as an attack source. By default, the alarm threshold is 60 pps.

Procedure

- Step 1** Run the **display auto-defend attack-source detail** command to check the detected attack source and check whether it is an authorized user.
- Step 2** If the interface is attacked and it connects to only one user, you do not need to take any actions because the attack has been blocked. Go to Step 5.
- Step 3** If the interface connects to multiple users and some users initiate attacks, you can configure attack source tracing and set the action taken on attack packets to deny, or configure a traffic policy to discard attack packets.

Step 4 If only entries exist on the interface or entries cannot be determined, collect device configurations, alarms, and logs, and then contact technical support personnel.

Step 5 End.

----End

Related Information

None

3.3.122 ALM-3276800107 Auto-port-defend alarm

Description

SECE/4/STRACKPORT: OID [OID] An port attack occurred. (Interface=[OCTET], Protocol=[OCTET])

Port attack defense is started.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800107	Warning	securityServiceOrMechanismViolation(10)

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
Interface	Indicates the attack source interface.
Protocol	Indicates the protocol type of attack packets.

Impact on the System

Service performance degrades and CPU usage may raise.

Possible Causes

When the device detects attack packets on an interface, the device starts attack defense on the interface.

Procedure

- Step 1**
Check whether the attack actually occurs on the interface.
- Step 2**
If an attack actually occurs, locate the attack source. If no attack occurs, reconfigure the port attack defense function to ensure that valid protocol packets can be sent to the CPU.
- End**

Related Information

None

3.3.123 ALM-3276800108 User-packets-abnormal alarm

Description

SECE/4/USERABNORMAL: OID [OID] The rate of packets received by a board exceeds the average rate. (board=[OCTET], UserIp=[OCTET], PacketType=[OCTET], NormalRate=[OCTET], ActualRate=[INTEGER]pps)

The rate of packets received by an LPU exceeded the normal rate.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800108	Warning	Quality of service alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
board	Indicates the LPU slot ID.
user ip	Indicates the IP address of a user.
packet type	Indicates the user packet type.
normal rate	Indicates the normal rate of user packets.
actual rate	Indicates the actual rate of user packets.

Impact on the System

The rate of packets received by an LPU exceeds the normal rate. Excessive packets are dropped. As a result, valid user services are interrupted and device performance degrades.

Possible Causes

The rate of packets received by an LPU exceeded the normal rate.

Procedure

- If user services are not affected, the alarm does not need to be handled.
- If user services are interrupted, perform the following operations:
 - a. Run the **display anti-attack statistics tcp-syn** command to check whether TCP SYN flood attack occurs.
 - b. Run the **display this** command in the URL template view of an X series card to check whether other commands, except URL commands, have been executed. If so, delete these commands.
 - c. Check whether wireless-to-wired (wireless users access the AC, and are authenticated by the switch) is configured on a card except the X series card. If so, replace the card with an X series card. If not, no action is required.
 - d. If this alarm is repeatedly reported and the alarms contain the same user IP address, check whether this user can go online. If the user can go online, no action is required. If the user fails to go online, check whether this user is authorized.
 - e. If the alarm persists, collect alarm, log, and configuration information of the device, and contact technical support personnel.

Related Information

None

3.3.124 ALM-3276800109 Neighbor information is changed

Description

LLDP/4/NBRCHGTRAP: OID [OID] Neighbor information is changed.
(LldpStatsRemTablesInserts=[integer], LldpStatsRemTablesDeletes=[integer],
LldpStatsRemTablesDrops=[integer], LldpStatsRemTablesAgeouts=[integer])

This alarm is generated when a neighbor is added, deleted, discarded, or aged.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800109	Warning	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
LldpStatsRemTablesInserts	Indicates the number of new neighbors.
LldpStatsRemTablesDeletes	Indicates the number of neighbors that are deleted.
LldpStatsRemTablesDrops	Indicates the number of neighbors that are discarded because of insufficient space.
LldpStatsRemTablesAgeouts	Indicates the number of neighbors that are aged.

Impact on the System

This alarm is a notification of changes in the network topology for the NMS, and no action is required.

Possible Causes

Cause 1:

A neighbor is found.

Cause 2:

A neighbor is deleted.

Cause 3:

A neighbor is aged.

Cause 4:

A neighbor is discarded because of insufficient space.

Procedure

Step 1 Check the values of **LldpStatsRemTablesInserts**, **LldpStatsRemTablesDeletes**, **LldpStatsRemTablesDrops**, and **LldpStatsRemTablesAgeouts** in the alarm message.

- If the value of **LldpStatsRemTablesInserts** is not 0, go to Step 2.
- If the value of **LldpStatsRemTablesDeletes** is not 0, go to Step 3.
- If the value of **LldpStatsRemTablesDrops** is not 0, go to Step 4.
- If the value of **LldpStatsRemTablesAgeouts** is not 0, go to Step 5.

- Step 2** Neighbors are discovered, indicating that new devices are connected to the device or LLDP is enabled on some neighbors. This message is a normal notification and you do not need to handle it. Go to Step 6.
- Step 3** Some neighbors are deleted, indicating that LLDP is disabled on these neighbors or the neighbors are disconnected from the device. Check whether the administrator has disabled LLDP on these devices or disconnected these devices from the device.
- If the administrator has disabled LLDP on these devices or disconnected these devices from the device, go to Step 6.
 - If not, rectify the link fault and go to Step 6.
- Step 4** The number of neighbors reaches the maximum (4096 on the entire device and 256 on each port). It is recommended that you disable LLDP on some minor ports to save information about the new neighbors. Go to Step 6.
- Step 5** Some neighbors are deleted after their aging time expires, indicating that the links between the neighbors and the device are faulty. Rectify the link fault and go to Step 6.
- Step 6** End.
- End

Related Information

None

3.3.125 ALM-3276800110 Global LLDP is enabled

Description

LLDP/4/ENABLETRAP: OID [OID] Global LLDP is enabled.

This notification is sent to the NMS when LLDP is enabled globally.

This alarm is allowed by the alarm delay.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800110	Warning	Equipment alarm

Parameters

Name	Meaning
[OID]	Indicates the MIB object ID of the alarm.

Impact on the System

This alarm is a notification of the change of the network topology for the NMS, and does not affect services.

Possible Causes

The LLDP is enabled globally.

Procedure

This is a normal notification and no action is required.

Related Information

None

3.3.126 ALM-3276800111 Global LLDP is disabled

Description

LLDP/4/DISABLETRAP: OID [OID] Global LLDP is disabled.

This notification is sent to the NMS when the LLDP is disabled globally.

This alarm is allowed by the alarm delay.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800111	Warning	Equipment alarm

Parameters

Name	Meaning
[OID]	Indicates the MIB object ID of the alarm.

Impact on the System

This alarm is a notification of the change of the network topology for the NMS, and does not affect services.

Possible Causes

The LLDP is disabled globally.

Procedure

This is a normal notification and no action is required.

Related Information

None

3.3.127 ALM-3276800112 Local management address is changed

Description

LLDP/4/ADDCHGTRAP: OID [OID] Local management address is changed.
(LocManAddr=[STRING])

The LLDP management address of a device was changed.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800112	Warning	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
LocManAddr	Indicates the local LLDP management address.

Impact on the System

This alarm is a notification of the change of the network topology for the NMS, and does not affect services.

Possible Causes

- The LLDP management address of a device was changed by running the **lldp management-address** command manually.
- The **lldp management-address** command was not configured on the device, but IP addresses of some interfaces changed. As a result, the LLDP management address changed.

Procedure

- Step 1** Check whether the local LLDP management address is the same as the planned one.
- If so, this alarm is informational only, and no action is required.
 - If not, go to step 2.
- Step 2** Run the **lldp management-address** command in the system view, and configure the local LLDP management address to the planned IP address.
- End

Related Information

None

3.3.128 ALM-3276800113 The Rate of Received PDUs Exceeded the Threshold

Description

LLDP/4/RATEEXCESSIVE: OID [OID] The rate of received PDUs exceeded the threshold. (IfName=[STRING])

The LLDP packets received by an interface exceeded five in one second.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800113	Warning	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
IfName	Indicates the interface name.

Impact on the System

If the interface is attacked by LLDP packets, it may not receive LLDP packets sent by a neighbor device. As a result, the judgment of the network topology for the NMS will be affected.

Possible Causes

- The interface had more than five LLDP neighbors, and all neighbors sent LLDP packets to it simultaneously.
- The interface was attacked by LLDP packets.

Procedure

- Step 1** Run the **display lldp neighbor interface** *interface-type interface-number* command in any view to check the number of LLDP neighbors on the interface found in the alarm. The *n* in "*STRING* has *n* neighbor(s)" displayed in the first line is the number.
- If *n* ranges from 0 to 5, the interface is attacked by LLDP packets. Go to step 2.
 - If *n* is greater than 5, the alarm cause cannot be determined. Go to step 2.
- Step 2** Run the **capture-packet interface** *interface-type interface-number destination terminal* command in the system view to capture packets received by the *STRING* interface. Check whether two or more captured LLDP packets have the same source MAC address.
- If so, run the **mac-address blackhole** *mac-address* command in the system view to set this MAC address as a blackhole MAC address, and go to step 4.
 - If not, go to step 3.
- Step 3** Check whether the current LLDP neighbor relationships on this interface are needed.
- If so, this alarm is informational only, and no action is required.
 - If not, go to step 4.
- Step 4** Disconnect unnecessary LLDP neighbor relationships. If the neighbor relationships can be disconnected, run the **undo lldp enable** command on the neighbor's interface that establishes a neighbor relationship with the local device to disable the LLDP function, or run the **undo l2protocol-tunnel lldp enable** command to disable transparent transmission for LLDP packets on the intermediate device's interface that connects to the LLDP neighbor device.
- Step 5** If the alarm persists, collect alarm information and configuration information, and then contact technical support personnel.

----End

Related Information

None

3.3.129 ALM-3276800114 Co-Channel Interference Between APs Was Detected

Description

WLAN/4/AP_COCHANNEL_INTERFERENCE: OID [oid] The co-channel interference exceeds the alarm threshold.(APMAC=[OPAQUE], RadioID=[INTEGER],

APName=[OCTET], APChannel=[INTEGER], APID=[INTEGER], IntfBssId=[OPAQUE],
RSSI threshold percent=[INTEGER]%)

Co-channel interference between APs was detected.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800114	Warning	Equipment alarm

Parameters

Name	Meaning
oid	Indicates the MIB object ID of the alarm.
APMAC	Indicates the MAC address of an AP.
APName	Indicates the AP name.
RadioID	Indicates the radio ID.
APChannel	Indicates the channel of a monitoring AP.
APID	Indicates the AP ID.
BssId	Indicates the BSSID of the interfering AP.
RSSI threshold percent	Indicates the RSSI threshold value on an interface, in percentage.

Impact on the System

The packet loss rate increases, the data rate decreases, and even the services may be interrupted.

Possible Causes

The alarm threshold for co-channel interference was exceeded.

Procedure

- Step 1** Run the **display radio-2g-profile { all | name *profile-name* }** and **display radio-5g-profile { all | name *profile-name* }** commands to view the value of **Co-channel frequency interference threshold(%)** and check whether the alarm threshold for co-channel interference is configured properly. It is recommended that you set the alarm threshold for co-channel interference to 50.

- If so, go to Step 3.
- If not, go to Step 2.

Step 2 Run the **interference co-channel threshold** *threshold-value* command to configure a proper alarm threshold for co-channel interference. Then, check whether the alarm persists.

- If the alarm persists, go to Step 3.
- If the alarm is cleared, go to Step 5.

Step 3 If severe interference triggers local radio calibration, the channel and power are adjusted automatically. Then, check whether the alarm persists.

- If the alarm persists, go to Step 4.
- If the alarm is cleared, go to Step 5.

Step 4 Collect alarm messages, log messages, and configurations, and then contact the technical support personnel.

Step 5 End.

----End

Related Information

None

3.3.130 ALM-3276800115 Adjacent Channel Interference Between APs Was Detected

Description

WLAN/4/AP_ADJACENT_CHANNEL_INTERFERENCE: OID [OID] The adjacent-channel interference exceeds the alarm threshold.(APMAC=[OPAQUE], RadioID=[INTEGER],APName=[OCTET], APChannel=[INTEGER], APID=[INTEGER], IntfBssId=[OPAQUE], IntfChnl=[INTEGER], RSSI threshold percent=[INTEGER]%)

Adjacent-channel interference between APs was detected.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800115	Warning	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
APMAC	Indicates the MAC address of an AP.

Name	Meaning
Radioid	Indicates the radio ID.
APName	Indicates the AP name.
APChannel	Indicates the channel of a monitoring AP.
APID	Indicates the AP ID.
IntfBssid	Indicates the BSSID of the interfering AP.
IntfChnl	Indicates the channel of the interfering AP.
RSSI threshold percent	Indicates the RSSI threshold value on an interface, in percentage.

Impact on the System

The packet loss rate increases, the data rate decreases, and even the services may be interrupted.

Possible Causes

The alarm threshold for adjacent-channel interference was exceeded.

Procedure

- Step 1** Run the **display radio-2g-profile { all | name *profile-name* }** and **display radio-5g-profile { all | name *profile-name* }** commands to view the value of **Adjacent-channel frequency interference threshold(%)** and check whether the alarm threshold for adjacent-channel interference is configured properly. It is recommended that you set the alarm threshold for adjacent-channel interference to 50.
- If so, go to Step 3.
 - If not, go to Step 2.
- Step 2** Run the **interference adjacent-channel threshold *threshold-value*** command to configure a proper alarm threshold for adjacent-channel interference. Then, check whether the alarm persists.
- If so, go to Step 3.
 - If not, go to Step 5.
- Step 3** If severe interference triggers local radio calibration, the channel and power are adjusted automatically. Then, check whether the alarm persists.
- If so, go to Step 4.
 - If not, go to Step 5.

Step 4 Collect alarm messages, log messages, and configurations, and then contact the technical support personnel.

Step 5 End.

----End

Related Information

None

3.3.131 ALM-3276800116 Jam of station is detected notify

Description

WLAN/4/STA_INTERFERENCE: OID [OID] Jam of station is detected notify.
(APMAC=[OPAQUE], RadioID=[INTEGER], APName=[OCTET], APID=[INTEGER])

STA interference was detected.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800116	Warning	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
APMAC	Indicates the MAC address of an AP.
RadioID	Indicates the radio ID.
APName	Indicates the AP name.
APID	Indicates the AP ID.

Impact on the System

If the number of interfering STAs exceeds the alarm threshold, the AP service performance is degraded.

Possible Causes

The number of interfering STAs exceeded the alarm threshold.

Procedure

- Step 1** Run the **display radio-2g-profile { all | name *profile-name* }** and **display radio-5g-profile { all | name *profile-name* }** commands to view the value of **Station interference threshold** and check whether the alarm threshold for STA interference is configured properly. It is recommended that you set the alarm threshold for STA interference to 32.
- If so, go to Step 3.
 - If not, go to Step 2.
- Step 2** Run the **interference station threshold** command to set a proper alarm threshold for STA interference. Then, check whether the alarm persists.
- If so, go to Step 3.
 - If not, go to Step 5.
- Step 3** Keep the AP away from the STAs that cause interference to decrease the STA interference to be lower than the alarm threshold. Then, check whether the alarm persists.
- If so, go to Step 4.
 - If not, go to Step 5.
- Step 4** Collect alarm messages, log messages, and configurations, and then contact the technical support personnel.
- Step 5** End.
- End

Related Information

None

3.3.132 ALM-3276800117 Interference from Other Devices Is Detected

Description

WLAN/4/UNKNOWN_DEVICE_INTERFERENCE: OID [OID] Jam of Other devices is detected.(APMAC=[OPAQUE], RadioID=[INTEGER],APName=[OCTET], APID=[INTEGER])

Interference from other devices is detected.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800117	Warning	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
APMAC	Indicates the MAC address of an AP.
RadioID	Indicates the radio ID.
APName	Indicates the AP name.
APID	Indicates the AP ID.

Impact on the System

The packet loss rate increases, the data rate decreases, and even the services may be interrupted.

Possible Causes

Devices, except for the co-channel APs, adjacent-channel APs, and STAs, worked on the AP channel and interfered with the AP.

Procedure

- Step 1

If severe interference deteriorates the environment, it will trigger local radio calibration, and the APs will automatically adjust the channel and power. Then, check whether the alarm persists.
 - If so, go to Step 2.
 - If not, go to Step 3.
- Step 2

Collect alarm messages, log messages, and configurations, and then contact the technical support personnel.
- Step 3

End.
- End

Related Information

None

3.3.133 ALM-3276800118 AP radio is down notify

Description

WLAN/4/AP_RADIO_DOWN: OID [oid] AP radio is down notify.
(APMAC=[OPAQUE], RadioID=[INTEGER], APName=[OCTET], CauseId=[INTEGER], CauseStr=[OCTET], APID=[INTEGER])
A radio was down.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800118	Warning	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object of the alarm.
APMAC	Indicates the MAC address of an AP.
RadioID	Indicates the radio ID.
APName	Indicates the AP name.
CauseId	Indicates the index of the radio disconnection cause.
CauseStr	Indicates the cause for a radio failure. • Radio disabled due to command execution: A radio shutdown command is delivered. • Radio disabled due to an error: An error occurs. • Radio disabled due to calibration: Radio calibration is performed. • Radio disabled due to low power consumption: The power consumption is low. • Radio disabled due to 3GPP base station notification: The 3GPP base station sends a radio shutdown instruction.
APID	Indicates the AP ID.

Impact on the System

The services on the STA are interrupted.

Possible Causes

- The radio was shut down as configured.
- The radio was shut down by radio calibration.
- Due to insufficient AP power, the AP works in low-power state.
- The radio was shut down due to a system error.

Procedure

- Step 1** No action is required when **CauseStr** is **Radio disabled due to command execution**.
- Step 2** No action is required when **CauseStr** is **Radio disabled due to calibration**.
- Step 3** No action is required when **CauseStr** is **The 3GPP base station sends a radio shutdown instruction**.
- Step 4** Check whether the power of the PoE switch connected to the AP is sufficient when **CauseStr** is **Radio disabled due to low power consumption**.
- Step 5** Collect the alarm information, log information, and configuration information, and then contact technical support personnel when **CauseStr** is **Radio disabled due to an error** or **Unexpected reason**.
- Step 6** End.
- End

Related Information

None

3.3.134 ALM-3276800119 The Channel Usage by Roaming STAs Exceeds the Threshold

Description

WLAN/4/ROAM_CHANNEL_UTIL_EXCEED_THRESHOLD:OID [OID] AP roam channelutilization exceed threshold notify. (APMAC=[OPAQUE], RadioID=[INTEGER], APName=[OCTET],ChannelUtil=[INTEGER], APID=[INTEGER])

The AP generates the alarm when the channel usage by roaming STAs exceeds the alarm threshold.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800119	Warning	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
APMAC	Indicates the MAC address of an AP.
RadioID	Indicates the radio ID of the AP.

Name	Meaning
APName	Indicates the AP name.
ChannelUtil	Indicates the channel usage.
APID	Indicates the AP ID.

Impact on the System

New users cannot roam to the AP.

Possible Causes

The channel usage exceeds the alarm threshold when users roam to the AP.

Procedure

- Step 1

Run the **uac channel-utilization threshold threshold access** *access-threshold* [**roam** *roam-threshold*] command in the radio profile view to increase the upper limit on the number of roaming users. Then, check whether the alarm persists.

If so, go to Step 2.

If not, go to Step 3.
- Step 2

Collect alarm messages, log messages, and configurations, and then contact the technical support personnel.
- Step 3

End.

----End

Related Information

None

3.3.135 ALM-3276800120 Upload remote capture file notify

Description

WLAN/4/RADIO_UPLOAD_REMOTE_CAPTURE_FILE_RESULT:OID [OID] Upload remote capture file notify. (APMAC=[OPAQUE], APName=[STRING], RadioID=[INTEGER], Info = [OCTET], APID=[INTEGER])

This alarm describes upload results of remote packet capturing files.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800120	Warning	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
APMAC	Indicates the MAC address of an AP.
APName	Indicates the AP name.
RadioID	Indicates the radio ID of the AP.
Info	Indicates upload results of remote packet capturing files.
APID	Indicates the AP ID.

Impact on the System

None

Possible Causes

The AP has uploaded remote packet capturing files.

Procedure

No action is required.

Related Information

None

3.3.136 ALM-3276800121 The configuration of an AP is inconsistent with the actual attribute

Description

WLAN/4/AP_CONFIG_INCONSIST_WITH_ACTUAL:OID [OID] The AP configuration is inconsistent with the actual attribute. (APMAC=[OPAQUE], APName=[STRING], APID=[INTEGER], Config=[OCTET], Reason=[OCTET])

The configuration of an AP is inconsistent with the actual attribute.

 NOTE

This alarm is supported only by the AP8130DN, AP2010DN, AP4051TN, and AP4030TN.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800121	Warning	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object of the alarm.
APMAC	Indicates the AP's MAC address.
APName	Indicates the AP name.
APID	Indicates the AP ID.
Config	Indicates the configuration.
Reason	Indicates the reason for the configuration inconsistency.

Impact on the System

None

Possible Causes

The actual radio frequency band of an AP is different from that configured on the AC.

Procedure

Step 1 Change the AP's radio frequency band to the actual one. Check whether the alarm persists.

- If so, go to Step 2.
- If not, go to Step 3.

Step 2 Collect trap, log, and configuration information, and contact Huawei technical support personnel.

Step 3 End.

----End

Related Information

None

3.3.137 ALM-3276800122 Detected rogue devices

Description

WLAN/4/WIDS_DETECT_ROGUE_DEVICE:OID [OID] Detected rogue devices.
(Device count=[INTEGER])

The alarm is generated when rogue devices are detected.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800122	Warning	environmentalAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
Device count	Indicates the number of rogue devices.

Impact on the System

Rogue devices exist in the current air interface environment and may affect air interface performance.

Possible Causes

Rogue devices are detected.

Procedure

- Step 1** Check the number of rogue devices and impact on services.
- If only a few rogue devices exist and services are not affected, no action is required.
 - If services are affected, go to Step 2.
- Step 2** Run the **display wlan ids device-detected all** command to check all detected rogue devices.
- Step 3** Contain detected rogue devices and configure WIDS rogue device containment.
1. Enter the AP group radio view or AP radio view, and run the **wids contain enable** command to enable rogue device containment.
 2. Enter the WIDS profile view and run the **contain-mode** command to configure the rogue device containment mode for APs.

- Step 4** Check whether the alarm persists.
- If so, go to Step 6.
 - If not, go to Step 7.
- Step 5** Collect alarm, log, and configuration information, and contact technical support personnel.
- Step 6** End.
- End

Related Information

None

3.3.138 ALM-3276800123 Detected attack devices

Description

WLAN/4/WIDS_DETECT_ATTACK:OID [OID] Detected attack devices. (Device count=[INTEGER])

This alarm is generated when attack devices are detected.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800123	Warning	environmentalAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
Device count	Indicates the number of attack devices.

Impact on the System

Attack devices exist in the current air interface environment and may affect air interface performance.

Possible Causes

Attack devices are detected.

Procedure

- Step 1** Check the number of attack devices and impact on services.
- If only a few attack devices exist and services are not affected, no action is required.
 - If services are affected, go to Step 2.
- Step 2** Run the **display wlan ids attack-detected all** command to check all detected attack devices.
- Step 3** Run the **dynamic-blacklist enable** command in the WIDS profile view to enable the dynamic blacklist function.
- Step 4** Check whether the alarm persists.
- If so, go to Step 5.
 - If not, go to Step 6.
- Step 5** Collect alarm, log, and configuration information, and contact technical support personnel.
- Step 6** End.
- End

Related Information

None

3.3.139 ALM-3276800124 Detected non-Wi-Fi devices

Description

WLAN/4/WIDS_DETECT_NON_WIFI:OID [OID] Detected non-Wi-Fi devices. (Device count=[INTEGER])

This alarm is generated when non-Wi-Fi devices are detected.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800124	Warning	environmentalAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
Device count	Indicates the number of non-Wi-Fi devices.

Impact on the System

Non-Wi-Fi devices exist in the current air interface environment and may affect air interface performance.

Possible Causes

Non-Wi-Fi devices are detected.

Procedure

- Step 1** Check the number of non-Wi-Fi devices and impact on services.
- If only a few non-Wi-Fi devices exist and services are not affected, no action is required.
 - If services are affected, go to Step 2.
- Step 2** Run the **display wlan non-wifi-device all** command to check all detected non-Wi-Fi devices.
- Step 3** Set the radio calibration policy to **non-wifi** or change the AP's working channel to avoid interference of non-Wi-Fi devices.
- Step 4** Check whether the alarm persists.
- If so, go to Step 5.
 - If not, go to Step 6.
- Step 5** Collect alarm, log, and configuration information, and contact technical support personnel.
- Step 6** End.
- End

Related Information

None

3.3.140 ALM-3276800125 AP not support configured channel

Description

WLAN/4/AP_UNSUPPORT_CHANNEL:OID [OID] AP not support configured channel notify.(APMAC=[MacAddress],RadioID=[INTEGER], APName=[OCTET], CONFIGURED BANDWIDTH=[INTEGER], CONFIGURED CHANNEL1=[INTEGER], CONFIGURED CHANNEL2=[INTEGER], ACTUAL BANDWIDTH=[INTEGER], ACTUAL CHANNEL1=[INTEGER], ACTUAL CHANNEL2=[INTEGER], REASON=[OCTET], APID=[INTEGER])

The alarm was generated if the AP does not support the channel delivered by the AC.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800125	Warning	processingErrorAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
APMAC	Indicates the MAC address of an AP.
RadioID	Indicates the radio ID of the AP.
APName	Indicates the AP name.
CONFIGURED BANDWIDTH	Indicates the configured bandwidth.
CONFIGURED CHANNEL1	Indicates the configured channel.
CONFIGURED CHANNEL2	Indicates the configured second channel.
ACTUAL BANDWIDTH	Indicates the actual bandwidth.
ACTUAL CHANNEL1	Indicates the actual channel used.
ACTUAL CHANNEL2	Indicates the actual second channel used.
REASON	Indicates the alarm reason.
APID	Indicates the AP ID.

Impact on the System

The AP still works on the original channel. The configuration delivered from the AC does not take effect.

Possible Causes

The AP does not support the channel delivered by the AC.

Procedure

- Step 1** Check whether the AP goes online on a WDS network.
- If so, the AP does not support channel delivered. Go to Step 4.
 - If not, go to Step 2.

- Step 2** Check the channel supported by the AP and run the **channel { 20mhz | 40mhz-minus | 40mhz-plus | 80mhz | 160mhz } channel** or **channel 80+80mhz channel1 channel2** command to change the channel configured for the AP. Check whether the alarm persists.
- If so, go to Step 3.
 - If not, go to Step 4.
- Step 3** Collect alarm messages, log messages, and configurations, and then contact the technical support personnel.
- Step 4** End.
- End

Related Information

None

3.3.141 ALM-3276800126 The EIRP is unlawful due to high antenna gain

Description

WLAN/4/AP_UNLAWFUL_EIRP:OID [OID] The EIRP is unlawful due to high antenna gain.(APMAC=[OPAQUE], RadioID=[INTEGER], APName=[OCTET], ConfigAntennaGain=[INTEGER], LegitimateAntennaGain=[INTEGER], APID=[INTEGER], LegitimateEIRP=[INTEGER])

The AP power is unlawful due to high antenna gain.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800126	Warning	processingErrorAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
APMAC	Indicates the MAC address of an AP.
RadioID	Indicates the radio ID of the AP.
APName	Indicates the AP name.
ConfigAntennaGain	Indicates the configured antenna gain.

Name	Meaning
LegitimateAntennaGain	Indicates the maximum legitimate antenna gain of the current AP in the current state.
APID	Indicates the AP ID.
LegitimateEIRP	Indicates the legitimate channel power.

Impact on the System

None

Possible Causes

The current antenna gain is invalid.

Procedure

- Step 1

Collect alarm messages, log messages, and configurations, and then contact the technical support personnel.
- Step 2

End.
- End

Related Information

None

3.3.142 ALM-3276800127 Power of radio is changed

Description

WLAN/4/RADIO_POWER_CHANGE:OID [OID] Power of radio is changed.
(APMAC=[OPAQUE], RadioID=[INTEGER], APName=[OCTET], ACTUAL
POWER=[INTEGER], APID=[INTEGER])

The alarm is generated when the AP radio power was changed.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800127	Warning	processingErrorAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
APMAC	Indicates the MAC address of an AP.
RadioID	Indicates the radio ID of the AP.
APName	Indicates the AP name.
ACTUAL POWER	Indicates the actual power.
APID	Indicates the AP ID.

Impact on the System

None

Possible Causes

- Cause 1: A notification about the power configuration modification was sent to the AP.
- Cause 2: The global calibration was enabled.
- Cause 3: The local calibration was enabled.
- Cause 4: The periodic calibration was enabled.

Procedure

This alarm is informational only, and no action is required.

Related Information

None

3.3.143 ALM-3276800130 Indicates that the stack-port state has changed to up

Description

FSP/4/STACKPORT_UP: OID [OID] Stack-port [integer]/[integer] changes to up.

This alarm was sent to the NMS by the master switch when the logical stack port of a switch in the stack system was Up.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800130	Warning	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
[integer]	Stack ID of the device generating the alarm.
[integer]	ID of the logical stack port whose status changes on the device. This ID starts from 0.

Impact on the System

If the stack interface is Up, service interfaces in the stack system increase. Services, however, are not interrupted.

If the stack interface is Down, the stack system recalculates the ring-breaking point, and then refreshes the forwarding entries. In this case, services are transiently interrupted and automatically recover after the forwarding entries are refreshed.

Possible Causes

- 1. The switch in the stack system was powered on.
- 2. The running switch was added to the stack system.

Procedure

This alarm is informational only, and no action is required.

Related Information

None

3.3.144 ALM-3276800131 Indicates that the stack-port state has changed to down

Description

FSP/3/STACKPORT_DOWN: OID [OID] Stack-port [integer]/[integer] changes to down.

This alarm was sent to the NMS by the master switch when the logical stack port of a switch in the stack system was Down.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800131	Minor	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
[integer]	Stack ID of the device generating the alarm.
[integer]	ID of the logical stack port whose status changes on the device. This ID starts from 0.

Impact on the System

If the previous stack system is in a ring topology and the interface in the Down state just functions as the ring-breaking point, the topology may become a link topology. Services, however, are not affected. If the logical stack port in the Down state does not function as the ring-breaking point, the stack system refreshes the forwarding entries. In this case, services are transiently interrupted and automatically recover after the forwarding entries are refreshed.

If the previous stack system is in a link topology, services on the switch that is Down are interrupted and cannot recover until the switch is added to the stack system again.

Possible Causes

1. The switch in the stack system was powered off.
2. The stack cable was connected loosely or even removed.
3. The stack card was loosened.

Procedure

- Step 1** Check whether the switch was powered off.
- If it was powered off, power on it. The alarm handling ends.
 - If not, go to step 2.
- Step 2** Run the **display stack port** command to check whether physical member ports are Up.
- If so, collect alarm information and configuration information, and then contact technical support personnel.
 - If not, go to step 3.
- Step 3** Check whether the stack card is loose. If it is loose, install it securely and then run the **display stack port** command to check whether physical member ports are Up.
- If so, the alarm handling ends.
 - If not, rectify the fault according to **An Ethernet Interface Is Physically Down** in the product documentation of the corresponding device.
- End

Related Information

None

3.3.145 ALM-3276800132 Logical Ports of a Stack Were Connected Incorrectly.

Description

FSP/3/LOGPORT_ILLEGAL: OID [OID] Stack port [octet1] connects to [octet2], and there are port members of the same logic stack port ID.

The logical stack ports are connected in a wrong order. The switch requires that the member ports in logical stack port 1 be connected to the member ports in stack port 2.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800132	Minor	Communication alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
[octet1]	Indicates the local interface name.

Name	Meaning
[octet2]	Indicates the name of remote interface connected to the local interface.

Impact on the System

The stack cannot be set up or the link generating the alarm is unavailable.

Possible Causes

The logical stack ports are connected in a wrong order.

Procedure

- Step 1 Run the **display stack port** command to check member ports of logical stack ports.
- Step 2 Connect the member ports in the local logical stack port 1 to those in the remote logical stack port 2, and connect the member ports in the local logical stack port 2 to those in the remote logical stack port 1.
- End

Related Information

None

3.3.146 ALM-3276800133 Indicates a stack physical port link error

Description

FSP/3/PHYPORT_ILLEGAL: OID [OID] Stack ports [octet1] and [octet2] are in the same logical stack port, but connect to different switches.

The member ports in a logical stack port on the switch are connected to different switches. The switch requires that the member ports in the same logical stack port be connected to the same switch.

NOTE

Incorrect stack logical connection: When physical ports connecting two member switches belong the same logical stack port, for example, logical stack port 1 or 2, the alarm hwStackLogicStackPortLinkErr is generated, indicating an incorrect stack logical connection.

Incorrect stack physical connection: When physical ports belonging to the same logical stack port connect to two member switches, the alarm hwStackPhyStackPortLinkErr is generated, indicating an incorrect stack physical connection.

If a physical port in a logical stack port experiences both physical and logical connection errors, only the alarm hwStackLogicStackPortLinkErr is generated, indicating an incorrect stack logical connection.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800133	Minor	Communication alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
[octet1]	Name of one physical port of the local device.
[octet2]	Name of the other physical port of the local device.

Impact on the System

The stack cannot be set up or the link generating the alarm is unavailable.

Possible Causes

The member ports in a logical stack port on the switch are connected to different switches.

Procedure

- Step 1** Run the **display stack port** command to check member ports of logical stack ports.
- Step 2** Run the **display lldp neighbor brief** command to check the remote device and ports to which member ports are connected.
- Step 3** Check whether the member ports in a logical stack port are connected to different devices.
 - If so, connect all member ports in the logical stack port to the same device according to the stack port connection rule.
 - If not, collect alarm information and configuration information, and then contact technical support personnel.

----End

Related Information

None

3.3.147 ALM-3276800134 Indicates that the stack physical port state has changed to down

Description

FSP/3/STACKPORTISDOWN: OID [OID] Stack port [octet] state is down.

A member port that has been added to a logical stack port becomes Down.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800134	Minor	Communication alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
[octet]	Indicates the local interface name.

Impact on the System

None

Possible Causes

The member port is not connected.

Procedure

Check whether this port has been connected using a cable.

- If no, connect it using a cable. The alarm handling ends.
- If so, rectify the fault according to **An Ethernet Interface Is Physically Down** in the product documentation of the corresponding device.

Related Information

[3.3.148 ALM-3276800135 A Member Port that Has Been Added to a Logical Stack Port Becomes Up](#)

3.3.148 ALM-3276800135 A Member Port that Has Been Added to a Logical Stack Port Becomes Up

Description

FSP/4/STACKPORTISUP: OID [OID] Stack port [octet] state has changed to up.

A member port that has been added to a logical stack port becomes Up.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800135	Warning	Communication alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
[octet]	Indicates the name of the local interface.

Impact on the System

None

Possible Causes

A member port that has been added to a logical stack port becomes Up after the cable is connected correctly.

Procedure

This alarm is informational only, and no action is required.

Related Information

[3.3.147 ALM-3276800134 Indicates that the stack physical port state has changed to down](#)

3.3.149 ALM-3276800136 Indicates that the other vlan conflicts with stack reserved-vlan

Description

FSP/3/VLAN_CONFLICT: OID [OID] [octet] conflicts with the stack reserved VLAN.
(VlanId=[integer])

The service VLAN conflicts with the stack reserved VLAN.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800136	Minor	environmentalAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
[octet]	Indicates the services or protocols that conflict with the stack reserved VLAN.
[integer]	Indicates the stack reserved VLAN ID.

Impact on the System

The stack reserved VLAN has been used by other service modules. As a result, other devices cannot join the stack.

Possible Causes

When a master/standby switchover occurs in the stack or member switches in the stack restart, and the master switch becomes a standalone switch, the VLAN manually created by users or automatically created by protocols such as VCMP and GVRP is the same as the stack reserved VLAN ID.

Procedure

- Step 1** Run the **display stack** command to check the stack reserved VLAN ID.
- Step 2** Run the **display vlan summary** command to check the created VLANs. Determine whether the stack reserved VLAN has been created on the switch.
 - If so, go to step 3.
 - If not, collect alarm information and configuration information, and then contact technical support personnel.

Step 3 Check whether the stack reserved VLAN ID can be changed to another VLAN ID.

- If so, run the **stack reserved-vlan** *vlan-id* command to change the stack reserved VLAN ID.
- If not, go to step 4.

Step 4 Delete the created stack reserved VLAN ID.

- If the created stack reserved VLAN is **Static VLAN**, run the **undo vlan** *vlan-id* command to delete it.
- If the created stack reserved VLAN is **Dynamic VLAN**, run the **undo gvrp** command to disable the GVRP function.
- If the created stack reserved VLAN is **Rrpp reserved**, run the **control-vlan** command to change the control VLAN of RRPP.
- If the created stack reserved VLAN is **Sep reserved**, run the **control-vlan (SEP segment view)** command to change the control VLAN of SEP.

----End

3.3.150 ALM-3276800137 Indicates that the stack set up failed

Description

FSP/3/SETUPFAILURE: OID [OID] Failed to set up a stack. (LocalSlotID=[integer], PeerSlotID=[integer], Reason=[STRING])

A stack fails to be set up.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800137	Minor	Communication alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
LocalSlotID	Indicates the slot ID of the local stack member switch.
PeerSlotID	Indicates the slot ID of the remote stack member switch.
Reason	Indicates the reason why the stack fails to be set up.

Impact on the System

Services cannot run normally.

Possible Causes

- The switches cannot set up a stack because of a device model mismatch.
- The switches cannot set up a stack because ports on a dedicated stack card are connected to service ports.

Procedure

- Step 1** Check whether ports on a dedicated stack card are connected to service ports on the panel or a service card.
- If so, change the connections.
 - If not, go to step 2.
- Step 2** Run the **display device** command to check the switch model.
- Step 3** Use switches of the same model or different models that allow to set up a stack together based on **Stack Configuration Notes**.

----End

3.3.151 ALM-3276800138 Indicates that the device auto config stack port failed

Description

FSP/2/AUTOCONFIGFAILED: OID [OID] Failed to auto configure stack port.
(SlotID=[integer], Port=[octet], Reason=[STRING])

After a dedicated stack cable was connected to the port, this port did not automatically become a stack port.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800138	Major	environmentalAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
SlotID	Indicates the slot ID of the interface to which a dedicated stack cable is connected.

Name	Meaning
Port	Indicates the port to which a dedicated stack cable is connected.
Reason	Indicates the reason why this port did not automatically become a stack port.

Impact on the System

A stack cannot be set up using dedicated stack cables.

Possible Causes

- Reason 1: This port does not support dedicated stack cables.
- Reason 2: Ports %s to %s have service configuration.
- Reason 3: This port has service configuration.
- Reason 4: The logical stack port to which this port needs to be added already has the maximum number of member ports.
- Reason 5: The rate of this port is inconsistent with that of other stack member ports.
- Reason 6: This port uses a different chip than other stack member ports.
- Reason 7: The system power supply mode is incorrect.
- Reason 8: The indirectly connected AS mode has been configured on the switch.
- Reason 9: The downlink port has been configured as an uplink port.
- Reason 10: This port has been configured as a member port of an SVF fabric port.
- Reason 11: On an AS, this port has been configured to the independent mode.
- Reason 12: A UCL group has been created using the **ucl-group** command.

Procedure

- Reason 1: This port does not support dedicated stack cables.
Run the **display stack port auto-cable-info** command to view ports supporting dedicated stack cables and then connect the dedicated stack cable to such a port.
- Reason 2 and reason 3: Ports %s to %s have service configuration and this port has service configuration.
 - On ASs in an SVF system, ensure that there are no other configurations except the **shutdown** and **stp root-protection** command configurations on ports. Delete unnecessary configurations according to Configuring Services for an AS.
 - On cloud-managed devices, ensure that there are no other configurations except the **shutdown** and **trust dscp** command configurations on ports. Delete unnecessary configurations through a controller.

- On other devices, ensure that there are no other configurations except the **shutdown** command configuration on ports. Run the **display this** command in the interface view to view services configured on this interface.
- If other services need to be configured, connect the dedicated stack cable to another port that supports this cable. To check ports supporting dedicated stack cables, run the **display stack port auto-cable-info** command.
- If other services do not need to be configured, run the **clear configuration this** command in the interface view to clear the configuration of this interface.
- Reason 4: The logical stack port to which this port needs to be added already has the maximum number of member ports.
 - a. Run the **display stack port auto-cable-info** command to view the logical stack port to which this port needs to be added.
 - b. Run the **display stack port brief** command to view member ports in a logical stack port.
- If the port needs to be added to this logical stack port, delete unnecessary member ports from this logical stack port. The method is as follows: Run the **shutdown interface** { *interface-type interface-number1* [*to interface-type interface-number2*] } &<1-10> command in the logical stack port view to shut down specified member ports and then run the **undo port interface** { *interface-type interface-number1* [*to interface-type interface-number2*] } &<1-10> **enable** command to delete these member ports from this logical stack port.
- If the port does not need to be added to the logical stack port, connect the dedicated stack cable to another port that supports this cable. To check ports supporting dedicated stack cables, run the **display stack port auto-cable-info** command.
- Reason 5: The rate of this port is inconsistent with that of other stack member ports.
 - a. Run the **display stack port auto-cable-info** command to view the logical stack port to which this port needs to be added.
 - b. Run the **display stack port brief** command to view the rate of member ports in the logical stack port.
- If the port needs to be added to this logical stack port, delete member ports whose rate is inconsistent with the rate described in this alarm. The method is as follows: Run the **shutdown interface** { *interface-type interface-number1* [*to interface-type interface-number2*] } &<1-10> command in the logical stack port view to shut down specified member ports and then run the **undo port interface** { *interface-type interface-number1* [*to interface-type interface-number2*] } &<1-10> **enable** command to delete these member ports from this logical stack port.
- If the port does not need to be added to this logical stack port, connect the dedicated stack cable to another port that supports this cable. To check ports supporting dedicated stack cables, run the **display stack port auto-cable-info** command.
- Reason 6: This port uses a different chip than other stack member ports.

When one logical stack port contains two stack member ports, this logical stack port can contain only stack member ports 1 and 2, or 3 and 4. Based on

this restriction, modify the logical stack port configuration or connect the dedicated stack cable to another port supporting this cable.

- Reason 7: The system power supply mode is incorrect.
Run the **set power manage mode** command to set the energy-saving mode to any mode except **standby**.
- Reason 8: The indirectly connected AS mode has been configured on the switch.
 - a. Run the **uni-mng** command to enter the uni-mng view and run the **display this** command to check the fabric port to which ports having dedicated stack cables connected are added.
 - b. Run the **interface_fabric-port** command to enter the fabric port view.
 - c. Run the **undo port connect-type** command to restore the direct connection mode of the fabric port.
- Reason 9: The downlink port has been configured as an uplink port.
Run the **undo uni-mng up-direction fabric-port** command to restore the port as a downlink port.
- Reason 10: This port has been configured as a member port of an SVF fabric port.
 - a. Run the **uni-mng** command to enter the uni-mng view and run the **display this** command to check the fabric port to which ports having dedicated stack cables connected are added.
 - b. Run the **interface_fabric-port** command to enter the fabric port view.
 - c. Run the **undo port eth-trunk trunkmember** command to unbind this port from the fabric port.
- Reason 11: On an AS, this port has been configured to the independent mode.
 - a. Run the **uni-mng** command to enter the uni-mng view and run the **display this** command to check the fabric port to which ports having dedicated stack cables connected are added.
 - b. Run the **interface_fabric-port** command to enter the fabric port view.
 - c. Run the **undo port connect** command to restore the centralized mode.
- Reason 12: A UCL group has been created using the **ucl-group** command.
Run the **undo ucl-group all** command in the system view to delete all UCL groups.

3.3.152 ALM-3276800139 Indicates that the card types are different

Description

ENTITYTRAP/4/CARDINCONSISTENT: OID [OID] The card types are different. (Index=[INTEGER], EntityPhysicalIndex=[INTEGER], PhysicalName="[OCTET]", EntityTrapEntType=[INTEGER], EntityTrapFaultID=[INTEGER], EntityTrapReasonDescr="[OCTET]")

The CSS card types in the same chassis are different.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800139	Warning	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
Index	Indicates an index.
EntityPhysicalIndex	Indicates the physical entity index.
PhysicalName	Indicates the name of the physical entity where the alarm is generated.
EntityTrapEntType	Indicates the alarm type.
EntityTrapFaultID	Indicates the fault ID of the alarm, 148736.
EntityTrapReasonDescr	Indicates the alarm reason: The types of CSS cards in a chassis are different.

Impact on the System

If the service traffic exceeds the capability of 10GE cards, traffic forwarded between the two chassis will not be load-balanced evenly.

Possible Causes

The CSS card types in the same chassis are different.

Procedure

- Step 1** Run the **display device** command to view the card types with the **Sub** field 1 in the same chassis.
- If the CSS card types in the same chassis are different, go to step 2.
 - If the CSS card types in the same chassis are the same, ignore this alarm.
- Step 2** Replace the CSS card to ensure that the CSS card types in the same chassis are the same.
- End

Related Information

None

3.3.153 ALM-3276800140 Failed to restore the system configurations

Description

HWCM/2/RESTORE_CONFIGURATION_FAIL:OID [OID] Failed to restore system configurations.(ErrCode=[ErrorCode])

Failed to restore the system configurations.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800140	Major	processingErrorAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
ErrorCode	Indicates the error code.

Impact on the System

Configurations for current services are lost.

Possible Causes

The configuration database file was lost or damaged.

Procedure

- Step 1** Run the **display startup** command to check the startup configuration file. Determine whether the file exists and has correct configuration data.
- If the file exists and has correct configuration data, go to Step 2.
 - If the file does not exist or have correct configuration data, go to Step 4.
- Step 2** Run the **display configuration recover-result** command to check configuration restoration failure details.
- Step 3** Collect alarm information and configuration information, and then contact technical support personnel.
- Step 4** End.
- End

Related Information

None

3.3.154 ALM-3276800141 The device was cold started

Description

SNMP/4/COLDSTART:OID [OID] coldStart.

The device was cold started.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800141	Warning	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.

Impact on the System

The alarm, generated because of the device cold start, brings no adverse impact on the system.

Possible Causes

The device was cold started.

Procedure

This trap message is informational only, and no action is required.

Related Information

None

3.3.155 ALM-3276800142 The device was hot started, or the SNMP agent was enabled

Description

SNMP/4/WARMSTART:OID [OID] warmStart.

The device was hot started, or the SNMP agent was enabled.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800142	Warning	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.

Impact on the System

The alarm, generated because of the device warm start, brings no adverse impact on the system.

Possible Causes

- The device was hot started.
- The SNMP agent was enabled.

Procedure

This trap message is informational only, and no action is required.

Related Information

None

3.3.156 ALM-3276800148 This object indicates the change of NTP synchronization status

Description

NTP/1/NTP_TRAP_SYNCHRONIZE_STATUS: OID [OID] NTP synchronization state changed. (hwNtpState=[STRING], hwNtpSource=[STRING], hwNtpSourceVpnName=[STRING])

NTP synchronization status changed.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800148	Critical	Quality of service alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
hwNtpState	NTP clock synchronization status
hwNtpSource	IP address of the synchronization source
hwNtpSourceVpnName	VPN name of the synchronization source

Impact on the System

NTP status becomes unsynchronous.

Possible Causes

NTP status changed from synchronous to unsynchronous due to the following reasons:

- Cause 1: The system clock reset was configured.
- Cause 2: The specified peer was deleted.
- Cause 3: The specified peer was unreachable.
- Cause 4: The specified peer failed to be authenticated.
- Cause 5: The clock of the specified peer was not synchronized.
- Cause 6: The source stratum was greater than the local stratum.
- Cause 7: The clock service of the specified peer was disabled.
- Cause 8: The clock source stratum of the specified peer was increased.

Procedure

- Cause 1: The system clock reset was configured.
 - a. Specify a new clock and check whether NTP enters the synchronous state.
 - If NTP enters the synchronous state, go to Step 3.
 - If NTP does not enter the synchronous state, go to Step 2.
 - b. Collect alarm information and configuration information, and then contact technical support personnel.

- c. End.
- Cause 2: The specified peer was deleted.
 - a. Configure a substitute clock source and check whether NTP enters the synchronous state.
 - If NTP enters the synchronous state, go to Step 3.
 - If NTP does not enter the synchronous state, go to Step 2.
 - b. Collect alarm information and configuration information, and then contact technical support personnel.
 - c. End.
- Cause 3: The specified peer was unreachable.
 - a. Check the network connectivity between the clock and its peer.
 - If the network is unreachable, go to Step 3.
 - If the network is reachable, go to Step 2.
 - b. Specify a new clock source and check whether NTP enters the synchronous state.
 - If NTP enters the synchronous state, go to Step 4.
 - If NTP does not enter the synchronous state, go to Step 3.
 - c. Collect alarm information and configuration information, and then contact technical support personnel.
 - d. End.
- Cause 4: The specified peer failed to be authenticated.
 - a. Check whether NTP authentication has been configured for both the local and peer ends.
 - If NTP authentication has been configured for both the local and peer ends, go to Step 2.
 - If NTP authentication has not been configured for the local or peer end or for both ends, configure NTP authentication as required.
 - b. Check whether NTP authentication keys configured for the local and peer ends are the same.
 - If NTP authentication keys configured for the local and peer ends are the same, go to Step 3.
 - If NTP authentication keys configured for the local and peer ends are different, reconfigure the keys so that they are the same.
 - c. Collect alarm information and configuration information, and then contact technical support personnel.
 - d. End.
- Cause 5: The clock of the specified peer was not synchronized.
 - a. Configure a substitute clock source and check whether NTP enters the synchronous state.

- If NTP enters the synchronous state, go to Step 3.
 - If NTP does not enter the synchronous state, go to Step 2.
 - b. Collect alarm information and configuration information, and then contact technical support personnel.
 - c. End.
- Cause 6: The source stratum was greater than the local stratum.
 - a. Run the **display ntp status** command to check the local stratum.
 - If the local stratum is less than the source stratum, go to Step 2.
 - If the local stratum is greater than the source stratum, go to Step 3.
 - b. Configure a substitute clock source, ensuring that the source stratum is less than the local stratum. Check whether NTP enters the synchronous state.
 - If NTP enters the synchronous state, go to Step 4.
 - If NTP does not enter the synchronous state, go to Step 3.
 - c. Collect alarm information and configuration information, and then contact technical support personnel.
 - d. End.
- Cause 7: The clock service of the specified peer was disabled.
 - a. Configure a substitute clock source and check whether NTP enters the synchronous state.
 - If NTP enters the synchronous state, go to Step 3.
 - If NTP does not enter the synchronous state, go to Step 2.
 - b. Collect alarm information and configuration information, and then contact technical support personnel.
 - c. End.
- Cause 8: The clock source stratum of the specified peer was increased.
 - a. Configure a substitute clock source and check whether NTP enters the synchronous state.
 - If NTP enters the synchronous state, go to Step 3.
 - If NTP does not enter the synchronous state, go to Step 2.
 - b. Collect alarm information and configuration information, and then contact technical support personnel.
 - c. End.

Clearing

The system automatically clears the alarm. You do not need to manually clear it.

Related Information

None

3.3.157 ALM-3276800149 Detected rogue device

Description

WLAN/4/WIDS_DETECT_ROGUE_DEVICE:OID [OID] Detected rogue devices.
(Device count=[INTEGER])

The alarm is generated when rogue devices are detected.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800149	Warning	environmentalAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
Device count	Indicates the number of rogue devices.

Impact on the System

Rogue devices exist in the current air interface environment and may affect air interface performance.

Possible Causes

Rogue devices are detected.

Procedure

- Step 1** Check the number of rogue devices and impact on services.
- If only a few rogue devices exist and services are not affected, go to Step 3.
 - If services are affected, go to Step 2.
- Step 2** Run the **display wlan ids device-detected all** command to check all detected rogue devices
- Step 3** Contain detected rogue devices and configure WIDS rogue device containment.
1. Enter the AP group radio view or AP radio view, and run the **wids contain enable** command to enable rogue device containment.

2. Enter the WIDS profile view and run the **contain-mode** command to configure the rogue device containment mode for APs.

Step 4 Check whether the alarm persists.

- If so, go to Step 6.
- If not, go to Step 7.

Step 5 Collect alarm and configuration information, and contact technical support personnel.

Step 6 End.

----End

Related Information

None

3.3.158 ALM-3276800150 AP changes to fault

Description

WLAN/2/AP_FAULT:OID [OID] AP changes to fault. (APMAC=[OPAQUE], APTYPE=[STRING], APName=[STRING], APFAULTTIME=[INTEGER], APID=[INTEGER])

An AP goes offline.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800150	Major	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
APMAC	Indicates the MAC address of an AP.
APType	Indicates the AP type.
APName	Indicates the AP name.
APFAULTTIME	Indicates the number of times the AP goes offline.
APID	Indicates the AP ID.

Impact on the System

The AC cannot manage the AP, and the AP-related services cannot work properly.

Possible Causes

Cause 1: The AP is disconnected from the AC.

Cause 2: The AP is powered off.

Cause 3: The heartbeat packets between AP and AC are lost.

Cause 4: The AC licenses are insufficient.

Cause 5: The AC and AP versions do not match.

Procedure

Step 1 Check whether the AP is disconnected from the AC.

- If so, connect them.
- If not, go to Step 2.

Step 2 Check whether the AP is powered off.

- If so, power on the AP.
- If not, go to Step 3.

Step 3 Check whether the AP and AC can exchange heartbeat packets.

- If not, verify network connectivity.
- If so and the alarm still exists, go to Step 4.

Step 4 Run the **display license resource usage** command to check whether AC licenses are sufficient.

- If so, go to Step 5.
- If not, apply for more AC licenses.

Step 5 Run the **display ap all** command to check whether the AC and AP versions match.

- If so, go to Step 6.
- If not, upgrade the AC and AP to matching versions.

Step 6 Collect alarm messages, log messages, and configurations, and then contact the technical support personnel.

Step 7 End.

----End

3.3.159 ALM-3276800151 AP ping result

Description

WLAN/4/AP_PING_RESULT:OID [OID] AP ping result. (APMAC=[OPAQUE], APTYPE=[STRING], APName=[STRING], SuccessCount=[INTEGER], FailureCount=[INTEGER]. AverageResponseTime=[INTEGER]ms.

MinimumResponseTime=[INTEGER]ms, MaximumResponseTime=[INTEGER]ms, APID=[INTEGER])

The result of AP ping operations issued from the NMS to the AP is reported.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800151	Warning	event

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
APMAC	Indicates the MAC address of an AP.
APType	Indicates the AP type.
APName	Indicates the AP name.
SuccessCount	Indicates whether the latest AP ping operation succeeds and the number of successful ping operations. Only the result of the latest ping is kept.
FailureCount	Indicates whether the latest AP ping operation succeeds and the number of failed ping operations. Only the result of the latest ping is kept.
AverageResponseTime	Indicates the average response time when you query the result of an AP ping operation. The unit is milliseconds. Only the result of the latest ping is kept.
MinimumResponseTime	Indicates the minimum response time when you query the result of an AP ping operation. The unit is milliseconds. Only the result of the latest ping is kept.
MaximumResponseTime	Indicates the maximum response time when you query the result of an AP ping operation. The unit is milliseconds. Only the result of the latest ping is kept.
APID	Indicates the AP ID.

Impact on the System

None

Possible Causes

The AP ping operation issued from the NMS to the AP is finished.

Procedure

This alarm is informational only, and no action is required.

Related Information

None

3.3.160 ALM-3276800152 AP is committed over

Description

WLAN/4/AP_COMMIT_OVER:OID [OID] AP is committed over.
(APMAC=[OPAQUE], APName=[STRING], APID=[INTEGER])

The AP configuration was committed.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800152	Warning	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
APMAC	Indicates the MAC address of an AP.
APName	Indicates the AP name.
APID	Indicates the AP ID.

Impact on the System

None

Possible Causes

None

Procedure

This alarm is informational only, and no action is required.

Related Information

None

3.3.161 ALM-3276800153 The AP began to upgrade

Description

WLAN/4/AP_UPDATE_BEGIN:OID [OID] AP begins to update. Do not power off the AP during the upgrade. (APMAC=[OPAQUE], APName=[STRING], APID=[INTEGER])

The AP began to upgrade.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800153	Warning	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
APMAC	Indicates the MAC address of an AP.
APName	Indicates the AP name.
APID	Indicates the AP ID.

Impact on the System

None

Possible Causes

The AP was upgraded.

Procedure

This alarm is informational only, and no action is required.

Related Information

None

3.3.162 ALM-3276800154 AP upgrade finished

Description

WLAN/4/AP_UPDATE_RESULT:OID [OID] AP updates completely.
(APMAC=[OPAQUE],
APName=[STRING],UpdateResult=[INTEGER],UpdateTime=[OCTET],UpdateFileName=[OCTET],UpdateNextOper=[INTEGER], UpdateStatus=[STRING],
APID=[INTEGER])

AP upgrade finished.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800154	Warning	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
APMAC	Indicates the MAC address of an AP.
APName	Indicates the AP name.
UpdateResult	Indicates the AP upgrade result.
UpdateTime	Indicates the AP upgrade time.
UpdateFileName	Indicates the AP upgrade file name.
UpdateNextOper	Indicates the operation after upgrade.
UpdateStatus	Indicates the AP upgrade result status.
APID	Indicates the AP ID.

Impact on the System

Services will not be affected after the successful upgrade.

APs and AP-based services cannot work properly after the failed automatic upgrade.

APs cannot be updated to the new version after the failed online upgrade.
However, current services are not affected.

Possible Causes

AP upgrade finished or failed.

Procedure

- Step 1** Check the upgrade result according to alarm parameters.
- If AP upgrade succeeded, go to Step 10.
 - If AP upgrade failed, go to Step 2.
- Step 2** Run the **display ap update configuration** command to view the AP upgrade mode.
- If the FTP mode is used, go to Step 3.
 - If the AC mode is used, go to Step 6.
- Step 3** Run the **display ap update configuration** command to check whether the FTP upgrade mode is correctly configured.
- If not, run the **ap update ftp-server** command to modify the configuration. And then go to Step 8.
 - If so, go to Step 4.
- Step 4** Check whether an upgrade file exists on the FTP server.
- If not, store the correct files on the FTP server. And then go to Step 8.
 - If so, go to Step 5.
- Step 5** Check whether the network connection between the AP and FTP server works properly.
- If not, rectify the network fault, and try again. And then go to Step 8.
 - If so, go to Step 7.
- Step 6** Run the **dir** command to check whether there is an upgrade file in the flash memory on the AC.
- If not, load correct files to the AC. And then go to Step 8.
 - If so, go to Step 7.
- Step 7** Check whether upgrade files are correct.
- If not, reload or store these files, and try again. And then go to Step 8.
 - If so, go to Step 9.
- Step 8** Check whether the upgrade succeeds.
- If so, go to Step 10.
 - If not, go to Step 9.
- Step 9** Collect the alarm information, log information, and configuration information, and then contact technical support personnel.
- Step 10** End.
- End

Related Information

None

3.3.163 ALM-3276800155 Unauthorized AP record exists

Description

WLAN/4/UNAUTHORIZED_AP_RECORD_EXIST:OID [OID] Unauthorized AP record exists.(Record number=[INTEGER])

An unauthorized AP alarm exists.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800155	Warning	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
Record number	Indicates the number of APs failing authentication.

Impact on the System

Rogue APs occupy links.

Possible Causes

Cause 1: The AP authentication mode is set to MAC address authentication, but the AP is not added offline and its MAC address is not in the whitelist.

Cause 2: The AP authentication mode is set to SN authentication, but the AP is not added offline and its SN is not in the whitelist.

Procedure

Step 1 Add authorized APs to the whitelist (add SNs or MAC addresses to the whitelist according to the AP authentication mode). Then, check whether the alarm persists.

- If so, go to Step 2.
- If not, go to Step 3.

- Step 2** Collect alarm messages, log messages, and configurations, and then contact the technical support personnel.
- Step 3** End.
- End

3.3.164 ALM-3276800156 The AP's Temperature Is Higher than the Upper Threshold

Description

WLAN/4/AP_TEMPERATURE_TOO_HIGH:OID [OID] The AP's temperature is too high. (APMAC=[OPAQUE], APName=[STRING], Temperature=[INTEGER]°C, APID=[INTEGER])

The AP's temperature is higher than the upper temperature threshold.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800156	Warning	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
APMAC	Indicates the MAC address of an AP.
APName	Indicates the AP name.
Temperature	Indicates the temperature of the AP. NOTE When the alarm is triggered on the R240D, R250D-E, AP2030DN, AP2050DN, AP2050DN-S, AP2050DN-E, AP3030DN, AP4030DN, AP4050DN, AP4051DN, AP4151DN, AP4050DN-S, AP4051DN-S, AP1050DN-S, AP430-E, AP4130DN, AP2030DN-S, AP2051DN, AP2051DN-S, AP2051DN-E, and R251D-E, the Temperature parameter indicates the alarm triggering threshold rather than the AP's actual temperature.
APID	Indicates the AP ID.

Impact on the System

The AP's temperature is higher than the upper temperature threshold.

- If the upper temperature threshold is not high, it has no impact on services.
- If the upper temperature threshold is high, the AP cannot work properly, affecting WLAN services.

Possible Causes

Cause 1: The upper temperature threshold is set to an improper value.

Cause 2: The ambient temperature is high.

Procedure

- Step 1** Run the **display ap-system-profile { all | name *profile-name* }** command to check whether the upper temperature threshold is set properly.
- If so, go to Step 3.
 - If not, go to Step 2.
- Step 2** Run the **high-temperature threshold *max-temperature*** command to set a proper upper temperature threshold.
- If the alarm persists, go to Step 3.
 - If the alarm is cleared, go to Step 5.
- Step 3** Reduce the ambient temperature by turning down air-conditioners or increase heat dissipation devices.
- If the alarm persists, go to Step 4.
 - If the alarm is cleared, go to Step 5.
- Step 4** Collect alarm messages, log messages, and configurations, and then contact the technical support personnel.
- Step 5** End.
- End

Related Information

[3.3.165 ALM-3276800157 The AP's temperature is too low](#)

3.3.165 ALM-3276800157 The AP's temperature is too low

Description

WLAN/4/AP_TEMPERATURE_TOO_LOW:OID [OID] The AP's temperature is too low. (APMAC=[OPAQUE], APName=[STRING], Temperature=[INTEGER]°C, APID=[INTEGER])

The AP's temperature is lower than the lower temperature threshold.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800157	Warning	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
APMAC	Indicates the MAC address of an AP.
APName	Indicates the AP name.
Temperature	Indicates the temperature of the AP.
APID	Indicates the AP ID.

Impact on the System

The AP's temperature is lower than the lower temperature threshold.

- If the lower temperature threshold is not low, the low AP temperature has no impact on services.
- If the lower temperature threshold is low, the AP cannot work properly, affecting WLAN services.

Possible Causes

Cause 1: The lower temperature threshold is set to an improper value.

Cause 2: The ambient temperature is too low.

Procedure

- Step 1** Run the **display ap-system-profile { all | name *profile-name* }** command to check whether the lower temperature threshold is set properly.
- If so, go to Step 3.
 - If not, go to Step 2.
- Step 2** Run the **low-temperature threshold *min-temperature*** command to set a proper lower temperature threshold.
- If the alarm persists, go to Step 3.
 - If the alarm is cleared, go to Step 5.
- Step 3** Increase the ambient temperature by turning up air-conditioners.
- If the alarm persists, go to Step 4.

- If the alarm is cleared, go to Step 5.

Step 4 Collect alarm messages, log messages, and configurations, and then contact the technical support personnel.

Step 5 End.

----End

Related Information

[3.3.164 ALM-3276800156 The AP's Temperature Is Higher than the Upper Threshold](#)

3.3.166 ALM-3276800158 AP CPU overload notify

Description

WLAN/4/AP_CPU_OVERLOAD: OID [OID] AP CPU overload notify.
(APMAC=[OPAQUE], APName=[STRING], ApCpuRate=[INTEGER], the top three thread CPU occupancy are [STRING], APID=[INTEGER])

The AP's CPU usage exceeds the upper threshold.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800158	Warning	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object of the alarm.
APMAC	Indicates the AP's MAC address.
APName	Indicates the AP name.
ApCpuRate	Indicates the AP's CPU usage.
[STRING2]	Indicates the top 3 threads with the highest CPU usage.
APID	Indicates the AP ID.

Impact on the System

The CPU usage exceeds the upper threshold. If the threshold is not high (for example, 50% or 60%), services are not affected. If the threshold is high (for example 90%), the AP reports the alarm, and packet loss may occur on the AP or the AP may be disconnected.

Possible Causes

Cause 1: The alarm threshold of the CPU usage is low.

Cause 2: The device provides too many services.

Cause 3: The device is attacked, causing high CPU usage.

Procedure

- Step 1** Run the **display ap-system-profile** command to check the alarm threshold for AP's CPU usage. Check whether the alarm threshold is set properly.
1. If so, go to [Step 3](#).
 2. If not, go to [Step 2](#).
- Step 2** Run the **cpu-usage threshold** command to set a proper alarm threshold for CPU usage. After that, check whether the alarm persists.
1. If this alarm persists, go to [Step 3](#).
 2. If the alarm is cleared, go to [Step 6](#).
- Step 3** Check whether the traffic volume is high. For example, check whether STAs frequently roam or a large number of STAs frequently go online or offline and check that the system runs normally.
1. If the traffic volume is high and the system runs normally, ignore the alarm.
 2. If the traffic volume is low, go to [Step 4](#).
- Step 4** Log in to the AP and run the **display cpu-usage** command in the diagnostic view to check the CPU usage of each task. Locate tasks with high CPU usage and delete unnecessary services or configurations to reduce the CPU usage.
1. If the alarm persists after some services are deleted, go to [Step 5](#).
 2. If the alarm is cleared, go to [Step 6](#).
- Step 5** Collect trap, log, and configuration information, as well as the CPU usage information in [Step 4](#), and contact technical support personnel.
- Step 6** If the alarm is cleared, no further action is required.

----End

Related Information

None

3.3.167 ALM-3276800159 AP memory overload notify

Description

WLAN/4/AP_MEM_OVERLOAD: OID [OID] AP memory overload notify.
(APMAC=[OPAQUE], APName=[STRING], ApMemRate=[INTEGER],
APID=[INTEGER])

The AP's memory usage exceeds the upper threshold.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800159	Warning	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object of the alarm.
APMAC	Indicates the AP's MAC address.
APName	Indicates the AP name.
ApMemRate	Indicates the AP's memory usage.
APID	Indicates the AP ID.

Impact on the System

The memory usage exceeds the upper threshold. If the threshold is not high (for example, 50% or 60%), services are not affected. If the threshold is high (for example 90%), the AP reports the alarm, and packet loss may occur on the AP or the AP may be disconnected.

Possible Causes

Cause 1: The memory alarm threshold is low.

Cause 2: The device provides too many services.

Procedure

- Step 1** Run the **display ap-system-profile** command to check the alarm threshold for memory usage. Check whether the alarm threshold is set properly.
- If so, go to step 3.
 - If not, go to step 2.
- Step 2** Run the **memory-usage threshold** command to set a proper alarm threshold for memory usage. After that, check whether the alarm persists.
- If the alarm persists, go to step 3.
 - If the alarm is cleared, go to step 5.
- Step 3** 3. Delete unnecessary services and configurations to reduce memory usage. Then check whether the alarm is cleared.
- If the alarm persists, go to step 4.
 - If the alarm is cleared, go to step 5.

Step 4 Collect alarms, logs, and configurations, and then contact technical support personnel.

Step 5 End.

----End

Related Information

None

3.3.168 ALM-3276800160 Dying gasp notify

Description

WLAN/4/AP_DYING_GASP: OID [OID] Dying gasp notify.(APMAC=[OPAQUE], APName=[STRING], APID=[INTEGER])

The dying gasp alarm was generated.



NOTE

This alarm is not supported by the AP4051TN, AP6052DN, AP7052DN, AP7152DN, AP7052DE, AP8050TN-HD, AP8082DN, or AP8182DN.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800160	Warning	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
APMAC	Indicates the MAC address of an AP.
APName	Indicates the AP name.
APID	Indicates the AP ID.

Impact on the System

The AP cannot work properly.

Possible Causes

The AP is powered off or its power supply is unstable.

Procedure

- Step 1** Check whether the power supply for the AP is normal.
- If the AP is powered off, go to Step 2.
 - If the power supply is working properly, go to Step 3.
- Step 2** Power on the power supply. Then, check whether the alarm persists.
- If so, go to Step 3.
 - If not, go to Step 6.
- Step 3** Check whether the AP's power supply is stable.
- If so, go to Step 4.
 - If not, go to Step 6.
- Step 4** Provide stable power supply to the AP. Then, check whether the alarm persists.
- If so, go to Step 5.
 - If not, go to Step 6.
- Step 5** Collect alarm messages, log messages, and configurations, and then contact the technical support personnel.
- Step 6** End.
- End

Related Information

None

3.3.169 ALM-3276800161 AC has system switched notify

Description

WLAN/4/AC_SYSTEM_SWITCH: OID [OID] AC has system switched notify.
(APMAC=[OPAQUE], APName=[STRING], APSN=[OCTET], SwitchType=[INTEGER],
APID=[INTEGER])

The active/standby switchover occurred on the AC.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800161	Warning	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
APMAC	Indicates the MAC address of an AP.
APName	Indicates the AP name.
APSN	Indicates the sequence number of an AP.
SwitchType	Indicates the switchover type of the AC.
APID	Indicates the AP ID.

Impact on the System

None

Possible Causes

The AC that is connected to the AP is faulty, or the network becomes unstable.

Procedure

- Step 1** Check the running status of the AC, which manages APs before the switchover.
- If the AC is reset, go to Step 4.
 - If the AC is not reset, go to Step 2.
- Step 2** Check whether the network is attacked or congested.
- If so, go to Step 3.
 - If not, go to Step 4.
- Step 3** Analyze the cause for network instability and rectify the fault based on the actual network situation.
- Step 4** Collect alarm messages, log messages, and configurations, and then contact the technical support personnel.
- Step 5** End.
- End

Related Information

None

3.3.170 ALM-3276800162 AP optical module received power is too high notify

Description

WLAN/4/AP_OPTICAL_RX_POWER_TOO_HIGH:OID [OID] AP optical module received power is too high notify. (APMAC=[OPAQUE], APName=[STRING], ApIfIndex=[INTEGER], Ap Optical RxPower=[INTEGER](0.1uw), ApEntityPhysicalName=[OCTET], APID=[INTEGER])

The receive power of the AP's optical module is higher than the upper power threshold.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800162	Warning	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
APMAC	Indicates the MAC address of an AP.
APName	Indicates the AP name.
ApIfIndex	Indicates the index of the AP interface on which the optical module is installed. Only the AD9430DN-24 and AD9431DN-24X support this object.
Ap Optical RxPower	Indicates the current receive power of the AP's optical module.
ApEntityPhysicalName	Indicates the name of the AP interface on which the optical module is installed. Only the AD9430DN-24 and AD9431DN-24X support this object.
APID	Indicates the AP ID.

Impact on the System

Services on the optical module are adversely affected, which probably leads to error codes, error packets, or even service interruption.

This alarm applies to Huawei certified optical modules only. For non-Huawei-certified optical modules, incorrect alarms may be generated.

Possible Causes

The receive power of the AP's optical module is higher than the upper power threshold.

Procedure

- Step 1** Check whether the type of the peer optical module matches that of the local optical module. For detailed matching rules, see **Hardware Failures > Interface Faults > An Optical Interface Cannot Turn Up** in the *Hardware Installation and Maintenance Guide* of the corresponding AP model.
- If so, go to Step 3.
 - If not, go to Step 2.
- Step 2** Replace the peer optical module with one matching the type of the local one. Then, check whether the alarm persists.
- If so, go to Step 3.
 - If not, go to Step 6.
- Step 3** Check whether the optical module is a Huawei certified optical module.
- If so, go to Step 5.
 - If not, go to Step 4.
- Step 4** Replace the optical module with a Huawei certified optical module. Then, check whether the alarm persists.
- If so, go to Step 5.
 - If not, go to Step 6.
- Step 5** Collect alarm messages, log messages, and configurations, and then contact the technical support personnel.
- Step 6** End.
- End

Related Information

[3.3.172 ALM-3276800164 AP optical module received power is too low notify](#)

3.3.171 ALM-3276800163 AP optical module temperature is too high notify

Description

WLAN/4/AP_OPTICAL_TEMPERATURE_TOO_HIGH:OID [OID] AP optical module temperature is too high notify. (APMAC=[MacAddress], APName=[STRING], ApIfIndex=[INTEGER], Ap Optical Temperature=[INTEGER]°C, ApEntityPhysicalName=[OCTET], APID=[INTEGER])

The temperature of AP's optical module is higher than the upper temperature threshold.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800163	Warning	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
APMAC	Indicates the MAC address of an AP.
APName	Indicates the AP name.
ApIfIndex	Indicates the index of the AP interface on which the optical module is installed. Only the AD9430DN-24 and AD9431DN-24X support this object.
Ap Optical Temperature	Indicates the temperature of the AP's optical module.
ApEntityPhysicalName	Indicates the name of the AP interface on which the optical module is installed. Only the AD9430DN-24 and AD9431DN-24X support this object.
APID	Indicates the AP ID.

Impact on the System

None

Possible Causes

The temperature of AP's optical module is higher than the upper temperature threshold.

Procedure

- Step 1** Reduce service traffic on the AP.
- If the alarm persists, go to Step 4.

- If the alarm is cleared, go to Step 5.

Step 2 Collect alarm messages, log messages, and configurations, and then contact the technical support personnel.

Step 3 End.

----End

Related Information

[3.3.173 ALM-3276800165 AP optical module temperature is too low notify](#)

3.3.172 ALM-3276800164 AP optical module received power is too low notify

Description

WLAN/4/AP_OPTICAL_RX_POWER_TOO_LOW:OID [OID] AP optical module received power is too low notify. (APMAC=[MacAddress], APName=[STRING], ApIfIndex=[INTEGER], Ap Optical RxPower=[INTEGER](0.1uw), ApEntityPhysicalName=[OCTET], APID=[INTEGER])

The receive power of the AP's optical module is lower than the lower power threshold.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800164	Warning	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
APMAC	Indicates the MAC address of an AP.
APName	Indicates the AP name.
ApIfIndex	Indicates the index of the AP interface on which the optical module is installed. Only the AD9430DN-24 and AD9431DN-24X support this object.
Ap Optical RxPower	Indicates the current receive power of the AP's optical module.

Name	Meaning
ApEntityPhysicalName	Indicates the name of the AP interface on which the optical module is installed. Only the AD9430DN-24 and AD9431DN-24X support this object.
APID	Indicates the AP ID.

Impact on the System

Services on the optical module are adversely affected, which probably leads to error codes, error packets, or even service interruption.

This alarm applies to Huawei certified optical modules only. For non-Huawei-certified optical modules, incorrect alarms may be generated.

Possible Causes

The receive power of the AP's optical module is lower than the lower power threshold.

Procedure

- Step 1** Check whether the type of the peer optical module matches that of the local optical module. For detailed matching rules, see **Hardware Failures > Interface Faults > An Optical Interface Cannot Turn Up** in the *Hardware Installation and Maintenance Guide* of the corresponding AP model.
- If so, go to Step 3.
 - If not, go to Step 2.
- Step 2** Replace the peer optical module with one matching the type of the local one. Then, check whether the alarm persists.
- If so, go to Step 3.
 - If not, go to Step 6.
- Step 3** Check whether the optical module is a Huawei certified optical module.
- If so, go to Step 5.
 - If not, go to Step 4.
- Step 4** Replace the optical module with a Huawei certified optical module. Then, check whether the alarm persists.
- If so, go to Step 5.
 - If not, go to Step 6.
- Step 5** Collect alarm messages, log messages, and configurations, and then contact the technical support personnel.

Step 6 End.
----End

Related Information

3.3.170 ALM-3276800162 AP optical module received power is too high notify

3.3.173 ALM-3276800165 AP optical module temperature is too low notify

Description

WLAN/4/AP_OPTICAL_TEMPERATURE_TOO_LOW:OID [OID] AP optical module temperature is too low notify. (APMAC=[MacAddress], APName=[STRING], ApIfIndex=[INTEGER], Ap Optical Temperature=[INTEGER]°C, ApEntityPhysicalName=[OCTET], APID=[INTEGER])

The temperature of AP's optical module is lower than the lower temperature threshold.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800165	Warning	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
APMAC	Indicates the MAC address of an AP.
APName	Indicates the AP name.
ApIfIndex	Indicates the index of the AP interface on which the optical module is installed. Only the AD9430DN-24 and AD9431DN-24X support this object.
Ap Optical Temperature	Indicates the temperature of the AP's optical module.

Name	Meaning
ApEntityPhysicalName	Indicates the name of the AP interface on which the optical module is installed. Only the AD9430DN-24 and AD9431DN-24X support this object.
APID	Indicates the AP ID.

Impact on the System

None

Possible Causes

The temperature of AP's optical module is lower than the lower temperature threshold.

Procedure

Step 1 Add service traffic on the AP.

- If the alarm persists, go to Step 4.
- If the alarm is cleared, go to Step 5.

Step 2 Collect alarm messages, log messages, and configurations, and then contact the technical support personnel.

Step 3 End.

----End

Related Information

[3.3.171 ALM-3276800163 AP optical module temperature is too high notify](#)

3.3.174 ALM-3276800166 AP not support configured country code notify

Description

WLAN/4/AP_UN SUPPORT_COUNTRY_CODE:OID [OID] AP not support configured country code notify.(APMAC=[MacAddress], APName=[STRING], COUNTRY CODE=[OCTET], APID=[INTEGER])

The AP does not support the country code configured on the AC.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800166	Warning	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
APMAC	Indicates the MAC address of an AP.
APName	Indicates the AP name.
COUNTRY CODE	Indicates the country code configured on the AP.
APID	Indicates the AP ID.

Impact on the System

The AP cannot get online.

Possible Causes

A country code not supported by the AP is configured on the AC.

Procedure

- Step 1** Run the **display regulatory-domain-profile** { **all** | **name** *profile-name* } command to check whether the country code configured on the AC is the same as that supported by the AP.
- If the country codes are the same, go to Step 3.
 - If the country codes are different, go to Step 2.
- Step 2** Run the **country-code** *country-code* command to set the country code of the AC to the one supported by the AP.
- If the alarm persists, go to Step 4.
 - If the alarm is cleared, go to Step 5.
- Step 3** Collect alarm messages, log messages, and configurations, and then contact the technical support personnel.
- Step 4** End.
- End

Related Information

None

3.3.175 ALM-3276800167 The AP cold boot

Description

WLAN/4/AP_COLD_BOOT:OID [OID] The AP cold boot. (APMAC=[MacAddress], AP TYPE=[OCTET], AP Sys Name=[OCTET], AP Sys Time=[OCTET], AP Alarm name=[OCTET], APID=[INTEGER])

The AP was cold started. After the AP was disconnected because of power-off, it connected to the AC again and operated properly.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800167	Warning	environmentalAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
APMAC	Indicates the MAC address of an AP.
AP TYPE	Indicates the AP type.
AP Sys Name	Indicates the AP name.
AP Sys Time	Indicates the time when the alarm is generated.
AP Alarm name	Indicates the alarm name.
APID	Indicates the AP ID.

Impact on the System

Services are interrupted after the AP is disconnected from the AC.

 NOTE

This alarm was triggered simultaneously with the alarm WLAN_1.3.6.1.4.1.2011.6.139.13.1.1.31 hwApColdBootRestoreTrap (the AP restored after a cold restart).

Possible Causes

The AP is powered on, goes online, and operates properly after an unexpected disconnection.

Procedure

- Step 1** Check whether the power supply of the AP is working properly. Then, check whether the alarm persists.
- If so, go to Step 2.
 - If not, go to Step 3.
- Step 2** Collect alarm messages, log messages, and configurations, and then contact the technical support personnel.
- Step 3** End.
- End

Related Information

None

3.3.176 ALM-3276800168 AP hot boot

Description

WLAN/4/AP_HOT_BOOT:OID [OID] AP hot boot. (APMAC=[OPAQUE], APTYPE=[OCTET], APName=[OCTET], APOccurTime=[OCTET], NotifyName=[OCTET], APID=[INTEGER])

An AP is hot started.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800168	Warning	environmentalAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
APMAC	Indicates the MAC address of an AP.
APType	Indicates the AP type.
APName	Indicates the AP name.

Name	Meaning
APOccurTime	Indicates the time when the alarm is generated.
NotifyName	Indicates the alarm name.
APID	Indicates the AP ID.

Impact on the System

The AP cannot work and its services are interrupted after a manual restart.

Possible Causes

The AP is manually restarted.

Procedure

- Step 1

Check whether the AP had been restarted. Then, check whether the alarm persists.
 - If so, go to Step 2.
 - If not, go to Step 3.
- Step 2

Collect alarm messages, log messages, and configurations, and then contact the technical support personnel.
- Step 3

End.
- End

Related Information

None

3.3.177 ALM-3276800169 AP CRC is abnormal notify

Description

WLAN/4/AP_CRC_TOO_HIGH:OID [OID] AP CRC is abnormal notify.
(APMAC=[OPAQUE], APName=[STRING], APCrcErrRate=[LONG]/10000,
PortType=[OCTET], PortID=[INTEGER], APID=[INTEGER])

The number of CRC error packets collected at a specified sampling interval exceeded the threshold.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800169	Warning	environmentalAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
APMAC	Indicates the MAC address of an AP.
APName	Indicates the AP name.
APCrcErrRate	Indicates the number of CRC error packets.
PortType	Indicates the AP port type.
PortID	Indicates the AP port number.
APID	Indicates the AP ID.

Impact on the System

None

Possible Causes

The number of CRC error packets collected at a specified sampling interval exceeded the threshold.

Procedure

- Step 1** Run the **display port-link-profile { all | name *profile-name* }** command to check whether the configured alarm threshold for CRC errors is proper.
- If so, go to Step 3.
 - If not, go to Step 2.
- Step 2** Run the **crc-alarm enable [high-threshold *high-threshold-value* | low-threshold *low-threshold-value*]*** command to set a proper alarm threshold for CRC errors.
- If the alarm persists, go to Step 3.
 - If the alarm is cleared, go to Step 4.
- Step 3** Collect alarm messages, log messages, and configurations, and then contact the technical support personnel.
- Step 4** End.
- End

3.3.178 ALM-3276800170 The U-boot Version Does Not Match the AP Version

Description

WLAN/4/AP_UBOOT_MISMATCH:OID [OID] AP uboot is not match AP version.
(APMac=[OPAQUE], APName=[STRING], APID=[INTEGER])

The U-boot version does not match the AP version.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800170	Warning	processingErrorAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
APMac	Indicates the MAC address of an AP.
APName	Indicates the AP name.
APID	Indicates the AP ID.

Impact on the System

The AP cannot work properly because of upgrade failures.

Possible Causes

The U-boot version does not match the AP version.

Procedure

- Step 1** Contact the technical support personnel to obtain the AP version matches the U-boot version.
- Step 2** Upgrade the AP according to the *AC Upgrade Guide*. Then, check whether the alarm persists.
 - If so, go to Step 3.
 - If not, go to Step 4.
- Step 3** Collect alarm messages, log messages, and configurations, and then contact the technical support personnel.

Step 4 End.

----End

Related Information

None

3.3.179 ALM-3276800171 Report ap name conflict

Description

WLAN/4/AP_NAME_CONFLICT:OID [OID] Report ap name conflict.
(APMAC=[OPAQUE], APReportName=[OCTET], APOccurTime=[OCTET],
APID=[INTEGER])

The name of a new online AP reported to the AC conflicts with that of an existing online AP.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800171	Warning	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
ApMac	Indicates the MAC address of an AP.
ApName	Indicates the AP name.
APOccurTime	Indicates the time when the alarm is generated.
APID	Indicates the AP ID.

Impact on the System

Two different APs use the same name, causing a failure in AP information query based on the AP name.

Possible Causes

The name configured on the AP conflicts with that of an online AP on the AC.

Procedure

- Step 1** Log in to the AP and run the **ap-rename** { **ap-name** *name* | **ap-mac** *ap-mac-address* | **ap-id** *ap-id* } **new-name** *ap-new-name* command to modify the name of the AP to prevent name conflict.
- Step 2** Restart the AP. Then, check whether the alarm persists.
- If so, go to Step 3.
 - If not, go to Step 4.
- Step 3** Collect alarm messages, log messages, and configurations, and then contact the technical support personnel.
- Step 4** End.
- End

Related Information

None

3.3.180 ALM-3276800172 AP License Notify

Description

WLAN/4/AP_NUM_REACH_LICENSE_UPLIMIT:OID [OID] AP License Notify. (Info = [OCTET])

AP specific license resources were insufficient (the number of online APs reached the maximum).

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800172	Warning	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
Info	Indicates AP license information.

Impact on the System

New APs cannot go online.

Possible Causes

The number of online APs reached the maximum value specified by the license.

Procedure

Step 1 Purchase new licenses or add new ACs to increase the maximum number of online APs. Then, check whether the alarm persists.

- If so, go to Step 2.
- If not, go to Step 3.

Step 2 Collect alarm messages, log messages, and configurations, and then contact the technical support personnel.

Step 3 End.

----End

Related Information

None

3.3.181 ALM-3276800173 AP IIC channel fault

Description

WLAN/4/AP_FMEA_FAULT_IIC_CHANNEL:OID [OID] AP IIC channel fault. (AP MAC=[OPAQUE], APName=[STRING], APID=[INTEGER])

The AP's IIC channel fails.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800173	Warning	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
APMAC	Indicates the MAC address of an AP.
APName	Indicates the AP name.
APID	Indicates the AP ID.

Impact on the System

The AP cannot properly work.

Possible Causes

The AP's IIC channel fails.

Procedure

Step 1 Check whether services are affected.

- If so, go to Step 2.
- If not, go to Step 4.

Step 2 Restart the AP. Then, check whether the alarm persists.

- If so, go to Step 3.
- If not, go to Step 5.

Step 3 Replace the faulty AP. Then, check whether the alarm persists.

- If so, go to Step 4.
- If not, go to Step 5.

Step 4 Collect alarm messages, log messages, and configurations, and then contact the technical support personnel.

Step 5 End.

----End

Related Information

None

3.3.182 ALM-3276800174 AP PHY CMOS fault

Description

WLAN/4/AP_FMEA_FAULT_PHY_CMOS:OID [oid] AP PHY CMOS fault.
(APMAC=[OPAQUE], APName=[STRING], APID=[INTEGER])

The AP's PHY chip fails.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800174	Warning	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
APMAC	Indicates the MAC address of an AP.
APName	Indicates the AP name.
APID	Indicates the AP ID.

Impact on the System

The AP cannot properly work.

Possible Causes

The AP's PHY chip fails.

Procedure

Step 1 Check whether services are affected.

- If so, go to Step 2.
- If not, go to Step 4.

Step 2 Restart the AP. Then, check whether the alarm persists.

- If so, go to Step 3.
- If not, go to Step 5.

Step 3 Replace the faulty AP. Then, check whether the alarm persists.

- If so, go to Step 4.
- If not, go to Step 5.

Step 4 Collect alarm messages, log messages, and configurations, and then contact the technical support personnel.

Step 5 End.

----End

Related Information

None

3.3.183 ALM-3276800175 AP FMEA fault

Description

WLAN/2/AP_FMEA_FAULT:OID [OID] AP FMEA fault. (APMAC=[OPAQUE], APName=[STRING], FaultID=[INTEGER], Index=[INTEGER], FaultInfo=[STRING], APID=[INTEGER])

The AP generates an alarm when a hardware fault occurs.

 NOTE

If a device generates a Failure Mode Effect Analysis (FMEA) alarm, the hardware circuit, module, or chip of the device becomes faulty.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800175	Warning	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
APMAC	Indicates the MAC address of the AP generating the hardware fault alarm.
APName	Indicates the name of the AP generating the hardware fault alarm.
FaultID	Indicates the index of the AP fault.
Index	Indicates the AP interface.
FaultInfo	Describes the AP fault.
APID	Indicates the AP ID.

Impact on the System

The AP cannot properly work.

Possible Causes

AP Fault Index	Possible Cause
1	The PHY chip is abnormal.

AP Fault Index	Possible Cause
2	The CPLD logic is abnormal.
3	The temperature sensor is abnormal.
4	The optical module is abnormal.
5	The Wi-Fi chip or PCIE is abnormal.
6	The LSW is abnormal.
7	Wi-Fi radio initialization failed.
8	Ethernet interface initialization failed.
9	The PSE input voltage is abnormal.
10	The PSE chip is abnormal.
11	An exception occurs on the USB flash drive.
12	The bad block rate for the NAND flash exceeds the threshold.
13	The voltage failed.
14	The double-edge connector failed.
15	The reset button failed.
16	The Bluetooth function failed.
17	The CPU failed.
18	The IIC of the PCA failed.

Procedure

Step 1 Check whether the value of **FaultID** is 4.

- If so, go to Step 2.
- If not, go to Step 6.

Step 2 Check whether the type of the peer optical module matches that of the local optical module. For detailed matching rules, see **Hardware Failures > Interface Faults > An Optical Interface Cannot Turn Up** in the *Hardware Installation and Maintenance Guide* of the corresponding AP model.

- If so, go to Step 4.
- If not, go to Step 3.

Step 3 Replace the peer optical module with one matching the type of the local one. Then, check whether the alarm persists.

- If so, go to Step 4.

- If not, go to Step 10.

Step 4 Check whether the optical module is a Huawei certified optical module.

- If so, go to Step 9.
- If not, go to Step 5.

Step 5 Replace the optical module with a Huawei certified optical module. Then, check whether the alarm persists.

- If so, go to Step 9.
- If not, go to Step 10.

Step 6 Check whether services are affected.

- If so, go to Step 7.
- If not, go to Step 9.

Step 7 Restart the AP. Then, check whether the alarm persists.

- If so, go to Step 8.
- If not, go to Step 10.

Step 8 Replace the faulty AP. Then, check whether the alarm persists.

- If so, go to Step 9.
- If not, go to Step 10.

Step 9 Collect alarm messages, log messages, and configurations, and then contact the technical support personnel.

Step 10 End.

----End

Related Information

None

3.3.184 ALM-3276800176 AP optical insert

Description

WLAN/4/AP_OPTICAL_INSERT:OID [OID] AP optical insert. (APMAC=[OPAQUE], APName=[STRING], IfIndex=[INTEGER], ApEntityPhysicalName=[OCTET], APID=[INTEGER])

An alarm is generated when an optical module is installed on an AP.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800176	Warning	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
APMAC	Indicates the MAC address of the AP on which an optical module is installed.
APName	Indicates the name of the AP on which an optical module is installed.
IfIndex	Indicates the index of the AP interface on which an optical module is installed.
ApEntityPhysicalName	Indicates the name of the AP interface on which the optical module is installed. Only the AD9430DN-24 and AD9431DN-24X support this object.
APID	Indicates the AP ID.

Impact on the System

None

Possible Causes

An optical module is installed on the AP.

Procedure

This alarm is informational only, and no action is required.

Related Information

[3.3.185 ALM-3276800177 AP optical remove](#)

3.3.185 ALM-3276800177 AP optical remove

Description

WLAN/4/AP_OPTICAL_REMOVE:OID [OID] AP optical remove.
 (APMAC=[OPAQUE], APName=[STRING], IfIndex=[INTEGER],
 ApEntityPhysicalName=[OCTET], APID=[INTEGER])

An alarm is generated when an optical module is removed from an AP.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800177	Warning	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
APMAC	Indicates the MAC address of the AP from which an optical module is removed.
APName	Indicates the name of the AP on which an optical module is removed.
IfIndex	Indicates the index of the AP interface on which an optical module is installed.
ApEntityPhysicalName	Indicates the name of the AP interface on which the optical module is installed. Only the AD9430DN-24 and AD9431DN-24X support this object.
APID	Indicates the AP ID.

Impact on the System

The AP cannot provide optical module functions.

Possible Causes

An optical module is removed from the AP.

Procedure

This alarm is informational only, and no action is required.

Related Information

[3.3.184 ALM-3276800176 AP optical insert](#)

3.3.186 ALM-3276800178 AP receive invalid arp new trap

Description

WLAN/4/AP_RECEIVED_INVALID_ARP_PACKET:OID [oid] AP received invalid arp packet notify.(APMAC=[OPAQUE], APName=[STRING], RadioID=[INTEGER], WlanID=[INTEGER], Drop Num=[INTEGER], APID=[INTEGER])

The AP receives invalid ARP packets.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800178	Warning	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
APMAC	Indicates the MAC address of an AP.
APName	Indicates the AP name.
RadioID	Indicates the ID of the radio under attack.
WlanID	Indicates the WLAN ID reporting the alarm.
Drop Num	Indicates the number of dropped packets.
APID	Indicates the AP ID.

Impact on the System

None

Possible Causes

The AP receives invalid ARP packets.

Procedure

Check whether the AP is attacked by ARP packets from rogue devices under assistant of technical support personnel.

Related Information

None

3.3.187 ALM-3276800179 AP software version is not match with AC software version

Description

WLAN/4/AP_SOFTWARE_VERSION_MISMATCH:OID [oid] AP software version is not match with AC software version.(APMAC=[OPAQUE], APName=[STRING], APTYPE=[OCTET], APSoftWareVersion=[OCTET], APID=[INTEGER])

The AP's version does not match the AC's.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800179	Warning	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
APMAC	Indicates the MAC address of an AP.
APName	Indicates the AP name.
APType	Indicates the AP type.
APSoftWareVersion	Indicates the software version of the AP.
APID	Indicates the AP ID.

Impact on the System

The AP cannot provide WLAN services.

Possible Causes

The AP's version does not match the AC's.

Procedure

Upgrade the AP to the target version according to the *AC Upgrade Guide*.

Related Information

None

3.3.188 ALM-3276800180 AP optical module transfer power is too high notify

Description

WLAN/4/AP_OPTICAL_TX_POWER_TOO_HIGH:OID [OID] AP optical module transfer power is too high notify. (APMAC=[OPAQUE], APName=[STRING], ApIfIndex=[INTEGER], Ap Optical TxPower=[INTEGER](0.1uw), ApEntityPhysicalName=[OCTET], APID=[INTEGER])

The transmit power of the AP's optical module exceeded the upper threshold.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800180	Warning	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
APMAC	Indicates the MAC address of an AP.
APName	Indicates the AP name.
ApIfIndex	Indicates the index of the AP interface on which the optical module is installed. Only the AD9430DN-24 and AD9431DN-24X support this object.
Ap Optical TxPower	Indicates the current transmit power of the AP's optical module.
ApEntityPhysicalName	Indicates the name of the AP interface on which the optical module is installed. Only the AD9430DN-24 and AD9431DN-24X support this object.
APID	Indicates the AP ID.

Impact on the System

Services on the optical module are adversely affected, which probably leads to error codes, error packets, or even service interruption.

This alarm applies to Huawei certified optical modules only. For non-Huawei-certified optical modules, incorrect alarms may be generated.

Possible Causes

The transmit power of the AP's optical module exceeded the upper threshold.

Procedure

- Step 1** Check whether the type of the peer optical module matches that of the local optical module. For detailed matching rules, see **Hardware Failures > Interface Faults > An Optical Interface Cannot Turn Up** in the *Hardware Installation and Maintenance Guide* of the corresponding AP model.
- If so, go to Step 3.
 - If not, go to Step 2.
- Step 2** Replace the peer optical module with one matching the type of the local one. Then, check whether the alarm persists.
- If so, go to Step 3.
 - If not, go to Step 6.
- Step 3** Check whether the optical module is a Huawei certified optical module.
- If so, go to Step 5.
 - If not, go to Step 4.
- Step 4** Replace the optical module with a Huawei certified optical module. Then, check whether the alarm persists.
- If so, go to Step 5.
 - If not, go to Step 6.
- Step 5** Collect alarm messages, log messages, and configurations, and then contact the technical support personnel.
- Step 6** End.
- End

Related Information

None

3.3.189 ALM-3276800181 AP optical module transfer power is too low notify

Description

WLAN/4/AP_OPTICAL_TX_POWER_TOO_LOW:OID [OID] AP optical module transfer power is too low notify. (APMAC=[MacAddress], APName=[STRING],

ApIfIndex=[INTEGER], Ap Optical TxPower=[INTEGER](0.1uw),
ApEntityPhysicalName=[OCTET], APID=[INTEGER])

The transmit power of the AP's optical module fell below the lower threshold.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800181	Warning	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
APMAC	Indicates the MAC address of an AP.
APName	Indicates the AP name.
ApIfIndex	Indicates the index of the AP interface on which the optical module is installed. Only the AD9430DN-24 and AD9431DN-24X support this object.
Ap Optical TxPower	Indicates the current transmit power of the AP's optical module.
ApEntityPhysicalName	Indicates the name of the AP interface on which the optical module is installed. Only the AD9430DN-24 and AD9431DN-24X support this object.
APID	Indicates the AP ID.

Impact on the System

Services on the optical module are adversely affected, which probably leads to error codes, error packets, or even service interruption.

This alarm applies to Huawei certified optical modules only. For non-Huawei-certified optical modules, incorrect alarms may be generated.

Possible Causes

The transmit power of the AP's optical module fell below the lower threshold.

Procedure

- Step 1** Check whether the type of the peer optical module matches that of the local optical module. For detailed matching rules, see **Hardware Failures > Interface Faults > An Optical Interface Cannot Turn Up** in the *Hardware Installation and Maintenance Guide* of the corresponding AP model.
- If so, go to Step 3.
 - If not, go to Step 2.
- Step 2** Replace the peer optical module with one matching the type of the local one. Then, check whether the alarm persists.
- If so, go to Step 3.
 - If not, go to Step 6.
- Step 3** Check whether the optical module is a Huawei certified optical module.
- If so, go to Step 5.
 - If not, go to Step 4.
- Step 4** Replace the optical module with a Huawei certified optical module. Then, check whether the alarm persists.
- If so, go to Step 5.
 - If not, go to Step 6.
- Step 5** Collect alarm messages, log messages, and configurations, and then contact the technical support personnel.
- Step 6** End.
- End

Related Information

None

3.3.190 ALM-3276800182 All functions of the fan module failed

Description

WLAN/4/AP_FAN_INVALID:OID [oid] All functions of the fan module failed.
(APMAC=[OPAQUE], APName=[STRING], ApFanIndex=[INTEGER],
ApEntityPhysicalName=[OCTET], APID=[INTEGER])

The alarm is generated when fans become faulty.

Only the AD9430DN-24 and AD9431DN-24X support this object.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800182	Warning	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
APMAC	Indicates the AP's MAC address.
APName	Indicates the AP name.
ApFanIndex	Indicates the interface index of the AP fan.
ApEntityPhysicalName	Indicates the AP interface name.
APID	Indicates the AP ID.

Impact on the System

The temperature of boards becomes high.

Possible Causes

Fans are faulty.

Procedure

Run the **display fan** command on AD9430DN-24 or AD9431DN-24X to check the fan status. Check whether the fan tray is registered and the fan speed is zero.

- If the fan tray is not registered, remove and install the fan tray.
- If the fan speed is zero, replace the fan.

If the fault persists, contact technical support personnel.

Related Information

None

3.3.191 ALM-3276800183 A storage card is removed

Description

WLAN/4/AP_STORAGE_CARD_REMOVE:OID [OID] A storage card is removed. (APMAC=[OPAQUE], APName=[STRING], ApStorageIndex=[INTEGER], ApStorageName=[OCTET], APID=[INTEGER])

This alarm is generated when a storage card is removed.

Only the AD9430DN-24 and AD9431DN-24X support this object.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800183	Warning	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
APMAC	Indicates the AP's MAC address.
APName	Indicates the AP name.
ApStorageIndex	Indicates the interface index of the storage card.
ApStorageName	Indicates the name of the storage card.
APID	Indicates the AP ID.

Impact on the System

If the alarm is displayed when the storage device is in position, the configuration file and log file may be lost.

Possible Causes

The storage device is pulled out.

Procedure

Check whether the storage device is removed. If not, contact the technical support personnel.

Related Information

None

3.3.192 ALM-3276800184 A storage card is inserted

Description

WLAN/4/AP_STORAGE_CARD_INSERT:OID [oid] A storage card is inserted.
(APMAC=[OPAQUE], APName=[STRING], ApStorageIndex=[INTEGER],
ApStorageName=[OCTET], APID=[INTEGER])

This alarm is generated when a storage card is inserted.

Only the AD9430DN-24 and AD9431DN-24X support this object.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800184	Warning	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
APMAC	Indicates the AP's MAC address.
APName	Indicates the AP name.
ApStorageIndex	Indicates the interface index of the storage card.
ApStorageName	Indicates the name of the storage card.
APID	Indicates the AP ID.

Impact on the System

None

Possible Causes

A storage device is inserted.

Procedure

Check whether the storage device is inserted. If not, contact the technical support personnel.

Related Information

None

3.3.193 ALM-3276800185 A port is powered off

Description

WLAN/4/AP_POE_POWER_OFF:OID [oid] A port is powered off.
(APMAC=[OPAQUE], APName=[STRING], ApIfIndex=[INTEGER],
ApEntityPhysicalName=[OCTET], APID=[INTEGER], Reason=[STRING])

The PD connected to the interface is powered off.

Only the AP4050DN-E, AP4050DN-HD, AP7050DN-E, AP7052DN, AP7152DN, AD9430DN-24, AD9431DN-24X and AD9430DN-12 support this alarm.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800185	Warning	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
APMAC	Indicates the AP's MAC address.
APName	Indicates the AP name.
ApIfIndex	Indicates the AP interface index.
ApEntityPhysicalName	Indicates the AP interface name.
APID	Indicates the AP ID.
Reason	Indicates the power-off reason.

Impact on the System

The PD connected to the interface is powered off and cannot work normally.

Possible Causes

Cause 1: The PD is removed.

Cause 2: The PD is faulty.

Cause 3: When the power is insufficient, the interface with higher priority preempts the power.

Cause 4: The interface is automatically powered off in the power-off time range.

Procedure

Step 1 Check whether the PD is removed.

- If so, go to step 2.
- If not, go to step 3.

Step 2 Install the PD and check whether the alarm is cleared.

- If so, go to step 11.
- If not, go to step 3.

Step 3 Check whether the power is sufficient.

- If so, go to step 7.
- If not, go to step 4.

Step 4 Check whether the priority of the interface is low.

- If so, go to step 5.
- If not, go to step 8.

Step 5 Check whether the interface priority is proper according to the requirements for the interface priority.

- If yes, use the **poe priority (AP wired port link profile view)** command to re-set the interface priority.
- If not, increase the PoE power.

Step 6 Check whether the alarm is cleared.

- If so, go to step 11.
- If not, go to step 7.

Step 7 Check whether the PD is faulty.

- If so, go to step 8.
- If not, go to step 9.

Step 8 Replace the PD and check whether the alarm is cleared.

- If so, go to step 11.
- If not, go to step 9.

Step 9 Check whether the interface is in the power-off time range.

- If so, go to step 11.
- If not, go to step 10.

Step 10 Contact technical support personnel.

Step 11 End

----End

Related Information

[3.3.194 ALM-3276800186 A port is powered on](#)

3.3.194 ALM-3276800186 A port is powered on

Description

WLAN/4/AP_POE_POWER_ON:OID [OID] A port is powered on.
(APMAC=[OPAQUE], APName=[STRING], ApIfIndex=[INTEGER],
ApEntityPhysicalName=[OCTET], APID=[INTEGER])

The interface meets the following power supply conditions:

- The power is sufficient.
- The PD is identified by the system.

Only the AP4050DN-E, AP4050DN-HD, AP7050DN-E, AP7052DN, AP7152DN, AD9430DN-24, AD9431DN-24X and AD9430DN-12 support this alarm.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800186	Warning	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
APMAC	Indicates the AP's MAC address.
APName	Indicates the AP name.
ApIfIndex	Indicates the AP interface index.
ApEntityPhysicalName	Indicates the AP interface name.
APID	Indicates the AP ID.

Impact on the System

Services are not affected.

Possible Causes

The alarm recovery message is generated after power-off.

Procedure

This alarm indicates that a fault is rectified, and no action is required.

Related Information

[3.3.193 ALM-3276800185 A port is powered off](#)

3.3.195 ALM-3276800187 A port detects connection of a PD

Description

WLAN/4/AP_POE_PD_CONNECTED:OID [OID] A port detects connection of a PD.
(APMAC=[OPAQUE], APName=[STRING], ApIfIndex=[INTEGER],
ApEntityPhysicalName=[OCTET], APID=[INTEGER])

The PD is connected to an interface.

Only the AP4050DN-E, AP4050DN-HD, AP7050DN-E, AP7052DN, AP7152DN,
AD9430DN-24, AD9431DN-24X and AD9430DN-12 support this alarm.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800187	Warning	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
APMAC	Indicates the AP's MAC address.
APName	Indicates the AP name.
ApIfIndex	Indicates the AP interface index.
ApEntityPhysicalName	Indicates the AP interface name.
APID	Indicates the AP ID.

Impact on the System

Services are not affected.

Possible Causes

The system detects a valid PD.

Procedure

A new PD is added. This alarm is informational and no action is required.

Related Information

None

3.3.196 ALM-3276800188 A port detects a PD whose current exceeds the threshold of the corresponding class

Description

WLAN/4/AP_POE_PD_CLASS_OVER_CURRENT:OID [OID] A port detects a PD whose current exceeds the threshold of the corresponding class.
(APMAC=[OPAQUE], APName=[STRING], ApIfIndex=[INTEGER], ApEntityPhysicalName=[OCTET], APID=[INTEGER])

The system detects that overcurrent occurs during PD classification and does not provide power for PDs.

Only the AP4050DN-E, AP4050DN-HD, AP7050DN-E, AP7052DN, AP7152DN, AD9430DN-24, AD9431DN-24X and AD9430DN-12 support this alarm.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800188	Warning	Communication alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
APMAC	Indicates the AP's MAC address.
APName	Indicates the AP name.
ApIfIndex	Indicates the AP interface index.
ApEntityPhysicalName	Indicates the AP interface name.
APID	Indicates the AP ID.

Impact on the System

Services are not affected.

Possible Causes

The PD does not comply with standards.

Procedure

- Step 1** You can run the **poe high-inrush enable (AP system profile view)** command in the AP system profile view to configure an interface to allow generation of the high pulse current. Then check whether the alarm is cleared.
- If yes, go to step 4.
 - If not, go to step 2.
- Step 2** Replace the PD and check whether the alarm is cleared.
- If yes, go to step 4.
 - If not, go to step 3.
- Step 3** Contact technical support personnel.
- Step 4** End.
- End

Related Information

None

3.3.197 ALM-3276800189 The port priority is different from the PD priority

Description

WLAN/4/AP_POE_PD_PRIORITY_DIFFERENT:OID [OID] The port priority is different from the PD priority. (APMAC=[OPAQUE], APName=[STRING], ApIfIndex=[INTEGER], ApEntityPhysicalName=[OCTET], ApPoePdPriority=[INTEGER], ApPoePortPriority=[INTEGER], APID=[INTEGER])

The interface priority is different from the PD priority.

Only the AP4050DN-E, AP4050DN-HD, AP7050DN-E, AP7052DN, AP7152DN, AD9430DN-24, AD9431DN-24X and AD9430DN-12 support this alarm.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800189	Warning	Quality of service alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
APMAC	Indicates the AP's MAC address.

Name	Meaning
APName	Indicates the AP name.
ApIfIndex	Indicates the AP interface index.
ApEntityPhysicalName	Indicates the AP interface name.
ApPoePdPriority	Indicates the PD priority.
ApPoePortPriority	Indicates the interface priority.
APID	Indicates the AP ID.

Impact on the System

Services are not affected.

Possible Causes

The interface priority is low, whereas the PD priority is high.

Procedure

- Step 1** Run the **poe priority (AP wired port link profile view)** command to change the interface priority to be higher than the PD priority. Then, check whether the alarm persists.
- If so, go to Step 2.
 - If not, go to Step 3.
- Step 2** Collect alarm messages, log messages, and configurations, and then contact the technical support personnel.
- Step 3** End.
- End

Related Information

None

3.3.198 ALM-3276800190 The power load of a PoE card exceeds the upper limit

Description

WLAN/4/AP_POE_POWER_OVER_UTILIZATION_THRESHOLD:OID [OID] The power load of a PoE card exceeds the upper limit. (APMAC=[OPAQUE], APName=[STRING], ApIfIndex=[INTEGER], ApEntityPhysicalName=[OCTET], ApPoeCurConsumPower=[INTEGER], ApPoeConsumPowerThreshold=[INTEGER], APID=[INTEGER])

The total PoE power consumption is greater than or equal to the alarm threshold.

Only the AP4050DN-E, AP4050DN-HD, AP7050DN-E, AP7052DN, AP7152DN, AD9430DN-24, AD9431DN-24X and AD9430DN-12 support this alarm.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800190	Warning	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
APMAC	Indicates the AP's MAC address.
APName	Indicates the AP name.
ApIfIndex	Indicates the AP interface index.
ApEntityPhysicalName	Indicates the AP interface name.
ApPoeCurConsumPower	Indicates the current consumed power.
ApPoeConsumPowerThreshold	Indicates the power threshold.
APID	Indicates the AP ID.

Impact on the System

If the alarm persists, all the PDs may be powered off because of insufficient power supply.

Possible Causes

The total power consumption of all the PDs is greater than or equal to the alarm threshold.

Procedure

Plan the network according to the system power supply. Increase priorities of important devices to prevent their power from being preempted. If the alarm persists, power off some PDs to ensure system reliability.

Related Information

None

3.3.199 ALM-3276800191 Interface has turned into DOWN state

Description

WLAN/4/AP_STP_AUTO_SHUTDOWN:OID [oid] Interface has turned into DOWN state. (APMAC=[OPAQUE], APName=[STRING], ApIfIndex=[INTEGER], ApEntityPhysicalName=[OCTET], APID=[INTEGER])

An alarm is generated when STP detects a local loopback and triggers port shutdown.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800191	Warning	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object of the alarm.
APMAC	Indicates the MAC address of the AP.
APName	Indicates the AP name.
ApIfIndex	Indicates the AP interface index.
ApEntityPhysicalName	Indicates the AP interface name.
APID	Indicates the AP ID.

Impact on the System

When STP detects a local loopback, it determines that a network storm occurs and will trigger shutdown of the local interface to prevent the storm from affecting services on the entire network; however, services on the shutdown interface will be interrupted.

Possible Causes

After STP detects a loopback on an interface, the device shuts down the interface to prevent a loop.

Procedure

- Step 1** Check whether local loopback is configured on the interface where the alarm is generated.

- Y=>4
- N=>2

Step 2 Check whether a hub is incorrectly connected on the network connected to the interface.

- Y=>5
- N=>3

Step 3 Collect alarm information, log information, and configuration information, and then contact technical support personnel.

Step 4 Delete configurations that cause the local loopback.

Step 5 Remove the self-looped cable.

Step 6 End

----End

Related Information

None

3.3.200 ALM-3276800192 The optical transceiver does not work normally

Description

WLAN/4/AP_OPTICAL_INVALID:OID [oid] The optical transceiver does not work normally. (APMAC=[OPAQUE], APName=[STRING], ApIfIndex=[INTEGER], ApEntityPhysicalName=[OCTET], hwWlanApOpticalFaultID=[INTEGER], APID=[INTEGER], hwWlanApOpticalFaultReason=[OCTET])

The AP's optical module is faulty.

Only the AD9430DN-24 and AD9431DN-24X support this object.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800192	Warning	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
APMAC	Indicates the AP's MAC address.

Name	Meaning
APName	Indicates the AP name.
ApIfIndex	Indicates the AP interface index.
ApEntityPhysicalName	Indicates the AP interface name.
hwWlanApOpticalFaultID	Indicates the fault ID of the AP's optical module.
APID	Indicates the AP ID.
hwWlanApOpticalFaultReason	Indicates the reason for the fault of the AP's optical module.

Impact on the System

Services will be interrupted.

Possible Causes

The rate of the optical module does not match the interface rate.

Procedure

Check the interface rate and replace the optical module with a proper one.

Related Information

None

3.3.201 ALM-3276800193 Online AP number exceeded card specific

Description

WLAN/4/AP_NUM_EXCEEDED: OID [OID] The number of online APs on the card has exceeded the maximum value. (Slot = [OCTET])

The number of APs going online on the card has exceeded the maximum.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800193	Warning	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
Slot	Indicates the slot ID.

Impact on the System

When the number of online APs exceeds the maximum, subsequent APs cannot go online.

Possible Causes

The number of APs going online on the card has exceeded the maximum.

Procedure

Expand the network capacity and plan the number of APs to be connected based on the network capacity.

Related Information

None

3.3.202 ALM-3276800194 The battery is low at the BLE site

Description

WLAN/4/BLE_LOW_POWER: OID [oid] The battery is low at the BLE site.
(BLEMAC=[OPAQUE])

The battery power of a BLE device is lower than the specified low power alarm threshold for BLE devices.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800194	Warning	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object of the alarm.

Name	Meaning
BLEMAC	Indicates the MAC address of a BLE device.

Impact on the System

If the battery is exhausted, a BLE device cannot work properly.

Possible Causes

The battery power of the BLE device is lower than the specified low power alarm threshold for BLE devices.

Procedure

Replace the battery of the BLE device.

Related Information

None

3.3.203 ALM-3276800195 An exception occurs at the BLE site

Description

WLAN/4/BLE_OFFLINE: OID [oid] An exception occurs at the BLE site.
(BLEMAC=[OPAQUE])

A BLE device gets offline.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800195	Warning	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object of the alarm.
BLEMAC	Indicates the MAC address of a BLE device.

Impact on the System

A BLE device cannot work normally after getting offline.

Possible Causes

The system cannot detect the signal from the BLE device for over 30 minutes.

Procedure

- Step 1** Check the operating status of the BLE device.
- If the BLE device works abnormally, go to step 2.
 - If the BLE device works normally, go to step 3.
- Step 2** Ensure that the BLE device can work normally.
- If the alarm persists, go to step 3.
 - If the alarm is cleared, go to step 4.
- Step 3** Collect information about alarms, logs, and configurations, and then contact technical support personnel.
- Step 4** This alarm is informational only, and no action is required.

----End

Related Information

None

3.3.204 ALM-3276800196 An IoT card is inserted

Description

WLAN/4/AP_IOT_CARD_INSERT:OID [OID] A iot card is inserted.
(APMAC=[OPAQUE], APName=[STRING], AplotCardId=[INTEGER],
APID=[INTEGER])

An IoT card is inserted.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800196	Warning	operationalViolation

Parameters

Name	Meaning
OID	ID of a MIB object.

Name	Meaning
APMAC	MAC address of an AP.
APName	Name of an AP.
AplotCardId	Number of the slot on an AP where an IoT card is installed.
APID	ID of an AP.

Impact on the System

If a card from Enjoyor is inserted, the AP restarts. Inserting a card from Prime Electronics & Satellitics Inc. has no impact on the system.

Possible Causes

An IoT card is inserted.

Procedure

This alarm is informational only, and no action is required.

Related Information

[3.3.211 ALM-3276800208 A iot card is removed](#)

3.3.205 ALM-3276800197 The AP's internal BLE module fails

Description

WLAN/4/INNER_BLE_BROKEN: OID [OID] The AP's internal BLE module fails.
(APMAC=[OPAQUE], APName=[STRING], APID=[INTEGER])

An AP's built-in Bluetooth module is faulty.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800197	Warning	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object of the alarm.
APMAC	Indicates the MAC address of an AP.

Name	Meaning
APName	Indicates the name of an AP.
APID	Indicates the ID of an AP.

Impact on the System

The AP's built-in Bluetooth module cannot work normally.

Possible Causes

The system did not detect heartbeat messages from the AP's built-in Bluetooth module for 32 seconds.

Procedure

- Step 1** Check the operating status of the AP's built-in Bluetooth module.
- If the AP's built-in Bluetooth module works abnormally, go to step 2.
 - If the AP's built-in Bluetooth module works normally, go to step 3.
- Step 2** Ensure that the AP's built-in Bluetooth module can work properly.
- If the alarm persists, go to step 3.
 - If the alarm is cleared, go to step 4.
- Step 3** Collect information about alarms, logs, and configurations, and then contact technical support personnel.
- Step 4** This alarm is informational only, and no action is required.

----End

Related Information

None

3.3.206 ALM-3276800198 Failed to start the server used by the IoT card

Description

WLAN/2/AP_IOT_SERVER_START_FAIL:OID [OID] Failed to start the server used by the IoT card. (Cause: The UDP port is occupied.) (APMAC=[OPAQUE], APName=[STRING], AplotCardId=[INTEGER], UdpPort=[INTEGER], APID=[INTEGER])

The server module on an AP for receiving data from the IoT card fails to start.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800198	Major	Communication alarm

Parameters

Name	Meaning
OID	ID of a MIB object.
APMAC	MAC address of an AP.
APName	Name of an AP.
AplotCardId	Number of the slot on an AP where an IoT card is installed.
UdpPort	UDP port number.
APID	ID of an AP.

Impact on the System

The server module on an AP for receiving data from the IoT card fails to start, and services are not available.

Possible Causes

The port used by the server module on the AP for receiving data from the IoT card is occupied.

Procedure

Change the IP address and port number.

Related Information

None

3.3.207 ALM-3276800199 SubFirmware is not match AP version

Description

WLAN/4/AP_SUBFIRMWARE_MISMATCH:OID [OID] SubFirmware is not match AP version. (APMAC=[OPAQUE], APName=[STRING], APSubFirmwareName=[STRING], APSubFirmware=[INTEGER], RealVersion=[STRING], ExpectVersion=[STRING], APID=[INTEGER])

The sub-firmware version on the AP mismatches.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800199	Warning	processingErrorAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object of the alarm.
APMAC	Indicates the AP's MAC address.
APName	Indicates the AP's name.
APSubFirmwareName	Indicates the AP's sub-firmware name.
APSubFirmware	Indicates the AP's sub-firmware number.
RealVersion	Indicates the actual version of the AP's sub-firmware.
APID	Indicates the AP ID.

Impact on the System

Version mismatch may cause faulty communication of the sub-firmware and affect functions of the sub-firmware.

Possible Causes

The sub-firmware upgrade fails and rolls back.

Procedure

- Step 1 Restart the AP and upgrade the sub-firmware again.
- Step 2 If the fault persists, contact technical support personnel.
- End

Related Information

None

3.3.208 ALM-3276800201 An AP detected that a Bluetooth tag was detached

Description

WLAN/4/BLE_DETACHED:OID [OID] The BLE site detached.
(BLEMAC=[OPAQUE(hex)])

An AP detected that a Bluetooth tag was detached.

NOTE

Only the AP2050DN-E, AP2051DN-E, AP4050DN-E, AP4051TN, AP6052DN, AP7050DE, AP7052DE, AP7052DN, AP4050DE-M, AP4050DE-M-S, AP4050DE-B-S, AP7060DN, AP6750-10T, AP7152DN, AP8050DN, AP8050DN-S, AP8050TN-HD, AP8082DN, AP8150DN, AP8182DN, R250D-E, and R251D-E support this alarm.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800201	Warning	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the ID of the alarm MIB object.
BLEMAC	Indicates the MAC address of a Bluetooth tag.

Impact on the System

After a Bluetooth tag is detached from an asset, the asset cannot be accurately located using Bluetooth location signals.

Possible Causes

The Bluetooth tag was detached from the asset.

Procedure

Check the Bluetooth tag location on the location server based on the Bluetooth tag location result. Find the Bluetooth tag and re-attach it to the asset.

Related Information

None

3.3.209 ALM-3276800202 The IoT Card Is Disconnected from the Server

Description

WLAN/2/IOT_CARD_DISCONNECT_SERVER:OID [OID] The IoT card is disconnected from the server. (APMAC=[OPAQUE], APName=[STRING], APID=[INTEGER], APlotCardId=[INTEGER], APlotCardType=[STRING])

An IoT card is disconnected from the server.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800202	Major	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the ID of a MIB object.
APMAC	Indicates the MAC address of an AP.
APName	Indicates the AP name.
APID	Indicates the AP ID.
APlotCardId	Indicates the ID of an IoT card.
APlotCardType	Indicates the type of an IoT card.

Impact on the System

An IoT card cannot communicate with the server.

Possible Causes

Cause 1: The link between the IoT card and server is disconnected, or the network configuration changes.

Cause 2: The IoT card is faulty.

Procedure

- Step 1** Check whether the network configuration between the IoT card and server is normal.
- If so, go to Step 3.

- If not, go to Step 2.

Step 2 Correct the network configuration and check whether the alarm is cleared.

- If so, go to Step 5.
- If not, go to Step 3.

Step 3 Replace the IoT card and check whether the alarm is cleared.

- If so, go to Step 5.
- If not, go to Step 4.

Step 4 Collect alarm and configuration information, and contact technical support personnel.

Step 5 End.

----End

Related Information

None

3.3.210 ALM-3276800203 The IoT Card Does Not Match the Configured Type

Description

WLAN/2/IOT_CARD_TYPE_MISMATCH:OID [OID] The IoT card does not match the configured type. (APMAC=[OPAQUE], APName=[STRING], APID=[INTEGER], APlotCardId=[INTEGER], APlotCardType=[STRING])

The IoT card type does not match the configuration.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800203	Major	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the ID of a MIB object.
APMAC	Indicates the MAC address of an AP.
APName	Indicates the AP name.
APID	Indicates the AP ID.
APlotCardId	Indicates the ID of an IoT card.

Name	Meaning
APlotCardType	Indicates the type of an IoT card.

Impact on the System

The AP cannot communicate with the IoT card.

Possible Causes

Cause 1: The configured IoT card type is incorrect.

Cause 2: The type of the inserted IoT card is incorrect.

Procedure

- Step 1** Check whether the IoT card type is correctly configured.
- If so, go to Step 3.
 - If not, go to Step 2.
- Step 2** Run the **card connect-type { ethernet | serial }** command to correctly configure the IoT card type. Check whether the alarm is cleared.
- If so, go to Step 5.
 - If not, go to Step 3.
- Step 3** Replace the IoT card with one of the correct type and check whether the alarm is cleared.
- If so, go to Step 5.
 - If not, go to Step 4.
- Step 4** Collect alarm and configuration information, and contact technical support personnel.
- Step 5** End.
- End

Related Information

None

3.3.211 ALM-3276800208 A iot card is removed

Description

WLAN/4/AP_IOT_CARD_REMOVE:OID [oid] A iot card is removed.
(APMAC=[OPAQUE], APName=[STRING], AplotCardId=[INTEGER],
APID=[INTEGER])

An IoT card is removed.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800208	Warning	operationalViolation

Parameters

Name	Meaning
OID	ID of a MIB object.
APMAC	MAC address of an AP.
APName	Name of an AP.
AplotCardId	Number of the slot on an AP where an IoT card is installed.
APID	ID of an AP.

Impact on the System

If a card from Enjoyor is removed, the AP restarts. Removing a card from Prime Electronics & Satellitics Inc. has no impact on the system.

Possible Causes

An IoT card is removed.

Procedure

Step 1 This alarm is informational only, and no action is required.

----End

Related Information

[3.3.204 ALM-3276800196 An IoT card is inserted](#)

3.3.212 ALM-3276800209 A port detects disconnection of a PD

Description

WLAN/4/AP_POE_PD_DISCONNECTED:OID [OID] A port detects disconnection of a PD. (APMAC=[OPAQUE], APName=[STRING], ApIfIndex=[INTEGER], ApEntityPhysicalName=[OCTET], APID=[INTEGER])

The PD is disconnected from an interface.

Only the AP4050DN-E, AP4050DN-HD, AP7050DN-E, AP7052DN, AP7152DN, AD9430DN-24, AD9431DN-24X and AD9430DN-12 support this alarm.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800209	Warning	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
APMAC	Indicates the AP's MAC address.
APName	Indicates the AP name.
ApIfIndex	Indicates the AP interface index.
ApEntityPhysicalName	Indicates the AP interface.
APID	Indicates the AP ID.

Impact on the System

The PD is unavailable and services are not affected.

Possible Causes

A valid PD is removed.

Procedure

Step 1 Check whether the PD is removed.

- If yes, go to step 3.
- If not, go to step 2.

Step 2 Reinstall the PD.

Step 3 End.

----End

Related Information

None

3.3.213 ALM-3276800210 The interface does not support the LRM optical module

Description

IFPDT/4/LRMABNORMAL: OID [OID] The interface does not support the LRM optical module. (InterfaceIndex=[INTEGER], InterfaceName=[OCTET])

The interface does not support LRM optical modules.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800210	Warning	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
InterfaceIndex	Indicates the interface index.
InterfaceName	Indicates the interface name.

Impact on the System

The transceiver is unavailable, and services on the corresponding interface are interrupted.

Possible Causes

An LRM optical module has been installed in a port that does not support LRM optical modules.

Procedure

- Step 1** Run the **display transceiver** command to check the type of the transceiver installed on the interface.
- If **Transceiver Type** is **10GBASE_LRM_SFP**, the optical module is an LRM optical module. Go to step 2.
 - If **Transceiver Type** is not **10GBASE_LRM_SFP**, the optical module is a non-LRM optical module. Go to step 3.
- Step 2** Replace the optical module with a non-LRM optical module.
- Step 3** Collect the configuration, alarm, and log information, and contact technical support personnel.

Step 4 End.

----End

3.3.214 ALM-3276800225 The current network cable quality is poor

Description

WLAN/4/SNR_ABNORMAL:OID [OID] The current network cable quality is poor, causing packet loss risks.(APMAC=[OPAQUE], APName=[STRING], InterfaceIndex=[INTEGER], InterfaceName=[OCTET], APID=[INTEGER])

The network cable quality is poor and packet loss may occur.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800225	Warning	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
APMAC	MAC address of an AP.
APName	AP name.
InterfaceIndex	Interface index.
InterfaceName	Interface name.
APID	AP ID.

Impact on the System

The network cable quality is poor and packet loss may occur.

Possible Causes

The network cable quality is poor or signal interference exists.

Procedure

- Replace the network cable with a high-quality network cable.
- Contact technical support personnel.

3.3.215 ALM-3276800226 A Failure to detect the network cable quality

Description

WLAN/6/SNR_DETECT_NOTSUPPORT:OID [OID] The port is Down, resulting in a failure to detect the network cable quality. (APMAC=[OPAQUE], APName=[STRING], InterfaceIndex=[INTEGER], InterfaceName=[OCTET], APID=[INTEGER])

The network cable quality is poor and packet loss may occur.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800226	Info	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
APMAC	Indicates the AP MAC address.
APName	Indicates the AP name.
InterfaceIndex	Interface index.
InterfaceName	Interface name.
APID	Indicates the AP ID.

Impact on the System

None

Possible Causes

The interface changes from Up to Down.

Procedure

This alarm is informational only and no action is required.

3.3.216 ALM-3276800227 AP power supply is insufficient

Description

WLAN/2/POWER_INSUFF:OID [OID] AP power supply is insufficient.
(APMAC=[OPAQUE], APName=[STRING], PowerWorkMode=[OCTET],
ExpectPowerWorkMode=[OCTET], APID=[INTEGER])

The AP power supply was insufficient.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800227	Major	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object of the alarm.
APMAC	Indicates the AP MAC address.
APName	Indicates the AP name.
PowerWorkMode	Indicates the actual power supply mode of the AP.
ExpectPowerWorkMode	Indicates the expected power supply mode of the AP.
APID	Indicates the AP ID.

Impact on the System

The AP restarts due to insufficient power supply.

Possible Causes

The power supply is insufficient for the AP.

Procedure

Step 1 Run the **lldp enable** command in the interface view to enable the LLDP function. In this way, the peer power supply device can identify the power supply standard of the local device and supply power as required.

- If the alarm persists, go to step 2.
- If the alarm is cleared, go to step 4.

- Step 2** Check the peer power supply device and ensure that the power supply standard meets the AP's power supply requirements.
- If the alarm persists, go to step 3.
 - If the alarm is cleared, go to step 4.
- Step 3** Collect alarm and configuration information, and contact technical support personnel.
- Step 4** End.
- End

Related Information

None

3.3.217 ALM-3276800228 An interface on an AP received a packet with an unauthorized MAC address

Description

WLAN/4/INSECURE_MAC:OID [OID] Interface receive insecure mac-address.
(APMAC=[OPAQUE], APName=[STRING], IllegalMAC=[OPAQUE],
VLANID=[INTEGER], InterfaceName=[OCTET], APID=[INTEGER])

An interface on an AP received a packet with an unauthorized MAC address.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800228	Warning	environmentalAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object of the alarm.
APMAC	Indicates the MAC address of the AP.
APName	Indicates the AP name.
IllegalMAC	Indicates the unauthorized MAC address.
VLANID	Indicates the VLAN ID.
InterfaceName	Indicates the interface name.
APID	Indicates the AP ID.

Impact on the System

None

Possible Causes

When the number of secure MAC addresses learned by the interface reached the maximum, the interface received a packet with an unauthorized MAC address.

Procedure

Check whether an unauthorized device is connected to the AP's interface.

Related Information

None

3.3.218 ALM-3276800229 The number of multicast and broadcast packets reported by an AP exceeded the alarm threshold

Description

WLAN/4/MCBC_EXCEED:OID [oid] The number of multicast and broadcast packets received on the AP exceeds the threshold 1000 pps for 10 seconds.
(APMAC=[OPAQUE], APName=[STRING], APID=[INTEGER])

The number of multicast and broadcast packets reported by an AP exceeded the alarm threshold.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800229	Warning	Quality of service alarm

Parameters

Name	Meaning
OID	Indicates the ID of the alarm MIB object.
APMAC	Indicates the MAC address of an AP.
APName	Indicates the AP name.
APID	Indicates the AP ID.

Impact on the System

If an AP reported too many multicast and broadcast packets, AP services are affected.

Possible Causes

The number of multicast and broadcast packets reported by the AP exceeded the alarm threshold.

Procedure

- Step 1** Check the networking, find senders of the multicast and broadcast packets, and optimize the networking. Check whether the alarm persists.
- If so, go to Step 2.
 - If not, go to Step 4.
- Step 2** Run the **traffic-optimize broadcast-suppression enable** command in the AP system profile view to enable the rate limit for broadcast packets and IGMP multicast packets on the AP. Check whether the alarm persists.
- If so, go to Step 3.
 - If not, go to Step 4.
- Step 3** Collect alarm, log, and configuration information, and contact technical support personnel.
- Step 4** End.
- End

3.3.219 ALM-3276800230 The AP type configured on the AC did not match the actual AP type

Description

WLAN/4/AP_TYPE_MISMATCH:OID [OID] The configured and reported AP types are different.(APMAC=[OPAQUE], APName=[STRING], APConfigType=[STRING], APActualType=[STRING], APID=[INTEGER])

The AP type configured on the AC did not match the actual AP type.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800230	Major	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the ID of the alarm MIB object.
APMAC	Indicates the AP's MAC address.
APName	Indicates the AP name.
APConfigType	Indicates the configured AP type.
APActualType	Indicates the actual AP type.
APID	Indicates the AP ID.

Impact on the System

The AP fails to go online.

Possible Causes

The AP type configured on the AC did not match the actual AP type.

Procedure

Configure the correct AP type.

3.3.220 ALM-3276800231 An AP detects that the Soft-GRE tunnel is Down

Description

WLAN/4/AP_DETECT_SOFTGRE_DOWN:OID [OID] AP detect softgre tunnel down notify.(APMAC=[OPAQUE], DstIP=[IPADDR], APName=[STRING], APID=[INTEGER])

An AP detects that the Soft-GRE tunnel is Down.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800231	Major	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the ID of the alarm MIB object.
APMAC	Indicates the MAC address of an AP.
DstIP	Indicates the destination IP address.
APName	Indicates the AP name.
APID	Indicates the AP ID.

Impact on the System

User traffic cannot be forwarded through the Soft-GRE tunnel.

Possible Causes

- After keepalive is enabled, the AP fails to ping the ME60.
- The Soft-GRE configuration is incorrect on the ME60. The ME60 does not respond to keepalive messages from the AP.
- The link between the AP and ME60 is torn down.

Procedure

- Step 1** Check whether the Soft-GRE function is enabled on the VE interface of the Soft-GRE tunnel.
 - Step 2** Check whether the IP address is correctly configured on the loopback interface.
 - Step 3** Check whether the Soft-GRE group is bound to the VE interface and loopback interface.
 - Step 4** Check whether the ME60 can ping the AP.
 - Step 5** Collect trap, log, and configuration information, and contact technical support personnel.
- End

3.3.221 ALM-3276800232 The AP version is not recommended for the current AC

Description

- WLAN/4/AP_VERSION_NOT_RECOMMENDED_TRAP:OID [OID] The AP version is not recommended for the current AC.
- The AP version is not recommended for the current AC.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800232	Warning	Quality of service alarm

Parameters

Name	Meaning
OID	Indicates the MIB object of the alarm.

Impact on the System

The load balancing effect may be affected.

Possible Causes

The AP version is not recommended for the current AC.

Procedure

Upgrade involved APs to the recommended version.

3.3.222 ALM-3276800234 The AP works in Limited mode due to insufficient power supply

Description

WLAN/4/AP_POWER_LIMITED: OID[OID] The AP works in Limited mode due to insufficient power supply.(APMAC=[OPAQUE], APName=[STRING], PowerWorkMode=[OCTET], ExpectPowerWorkMode=[OCTET], APID=[INTEGER])

The AP power supply is insufficient, and the AP works in Limited mode.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800234	Warning	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object of the alarm.

Name	Meaning
APMAC	Indicates the AP MAC address.
APName	Indicates the AP name.
PowerWorkMode	Indicates the actual power supply mode of the AP.
ExpectPowerWorkMode	Indicates the expected power supply mode of the AP.
APID	Indicates the AP ID.

Impact on the System

When an AP works with low power consumption, some component functions such as the USB and PoE out functions are disabled. In addition, radio power is reduced, or radios are disabled. For details, see the functions of APs using different power supply standards in **AP Management Configuration Guide****Managing the PoE Function of an AP****Understanding PoE** in the *S2720, S5700, and S6700 V200R019C00 Configuration Guide - WLAN-AC*.

Possible Causes

The device that supplies power to the AP does not meet the AP's power supply requirements.

Procedure

- Step 1** Run the **lldp enable** command in the interface view to enable the LLDP function. In this way, the peer power supply device can identify the power supply standard of the local device and supply power as required.
 - If the alarm persists, go to step 2.
 - If the alarm is cleared, go to step 4.
- Step 2** Check the peer power supply device and ensure that the power supply standard meets the AP's power supply requirements.
 - If the alarm persists, go to step 3.
 - If the alarm is cleared, go to step 4.
- Step 3** Collect alarm and configuration information, and contact technical support personnel.
- Step 4** End.
- End

Related Information

None

3.3.223 ALM-3276800235 The WAPI certificate is nearly expired

Description

WLAN/4/WAPI_CERT_NEARLY_EXPIRED: OID [OID] The WAPI certificate is nearly expired. (SecurityProfileName=[STRING], CertType=[STRING], CertFileName=[STRING], CertStartTime=[STRING], CertEndTime=[STRING])

The validity period of the WAPI certificate loaded to the security profile is less than 30 days.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800235	Warning	Quality of service alarm

Parameters

Name	Meaning
OID	Indicates the ID of a MIB object.
SecurityProfileName	Indicates the name of a security profile.
CertType	Indicates the type of a certificate. The value can be: - ac - asu - issuer
CertFileName	Indicates the name of a WAPI certificate file.
CertStartTime	Indicates the start time of WAPI certificate validity.
CertEndTime	Indicates the end time of WAPI certificate validity.

Impact on the System

After the WAPI certificate expires, users using this certificate cannot access the network.

Possible Causes

The validity period of the WAPI certificate loaded to the security profile is less than 30 days.

Procedure

- Step 1** Check whether the current system time is correct.
- If so, go to step 3.
 - If not, go to step 2.
- Step 2** Change the system time.
- If the alarm persists, go to step 3.
 - If the alarm is cleared, go to step 5.
- Step 3** Replace the certificate before it expires.
- If the alarm persists, go to step 4.
 - If the alarm is cleared, go to step 5.
- Step 4** Collect alarm, log, and configuration information, and contact technical support personnel.
- Step 5** End.
- End

Related Information

None

3.3.224 ALM-3276800236 The WAPI certificate is invalid

Description

WLAN/2/WAPI_CERT_INVALID: OID [OID] The WAPI certificate is invalid.
(SecurityProfileName=[STRING], CertType=[STRING], CertFileName=[STRING],
CertStartTime=[STRING], CertEndTime=[STRING])

The WAPI certificate loaded to the security profile expires.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800236	Major	Quality of service alarm

Parameters

Name	Meaning
OID	Indicates the ID of a MIB object.

Name	Meaning
SecurityProfileName	Indicates the name of a security profile.
CertType	Indicates the type of a certificate. The value can be: • ac • asu • issuer
CertFileName	Indicates the name of a WAPI certificate file.
CertStartTime	Indicates the start time of WAPI certificate validity.
CertEndTime	Indicates the end time of WAPI certificate validity.

Impact on the System

Users using this certificate cannot access the network.

Possible Causes

The WAPI certificate loaded to the security profile expires.

Procedure

Step 1 Check whether the current system time is correct.

- If so, go to step 3.
- If not, go to step 2.

Step 2 Change the system time.

- If the alarm persists, go to step 3.
- If the alarm is cleared, go to step 5.

Step 3 Replace the certificate.

- If the alarm persists, go to step 4.
- If the alarm is cleared, go to step 5.

Step 4 Collect alarm, log, and configuration information, and contact technical support personnel.

Step 5 End.

----End

Related Information

None

3.3.225 ALM-4289601623 Virtual license is approaching expiration date alert

Description

ENTITYTRAP/4/VLCS_NEAR_DEADLINE: OID [OID] Virtual license is near deadline, remain time is [INTEGER] days. (ItemName="[OCTET]")

The virtual license is about to expire.

Attribute

Alarm ID	Alarm Severity	Alarm Type
4289601623	Critical	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
INTEGER	Remaining validity duration, in days.
ItemName	Name of the control item.

Impact on the System

This alarm is for warning in advance without affecting the service.

Possible Causes

After the device is migrated to the cloud and a virtual license is activated on the device in a cloud scenario, the device is in Retrieving status and the alarm is triggered every day.

Procedure

Step 1 Check the validity period of the virtual license on the controller.

Step 2 Renew the license in time.

----End

3.3.226 ALM-4289601624 Virtual license has expired

Description

ENTITYTRAP/2/VLCS_EXPIRED: OID [OID] The virtual license has expired.
(ItemName="[OCTET]")

The virtual license has expired.

Attribute

Alarm ID	Alarm Severity	Alarm Type
4289601624	Major	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
ItemName	Name of the control item.

Impact on the System

The dynamic VXLAN tunnel of the device goes Down and the service becomes unavailable.

Possible Causes

The virtual license of the device has expired.

Procedure

Step 1 Check the validity period of the virtual license on the controller.

Step 2 Renew the license.

----End

Related Information

None

3.3.227 ALM-1099702272 Resource item is nearly used up

Description

GTL/2/RESOURCE_USEDUP:OID [OID] Resource item [item-name] is nearly used up.

The trap was generated when the percentage of the resources used by the service module was not less than the 90% which is defined by the license.

Attribute

Alarm ID	Alarm Severity	Alarm Type
1099702272	Major	environmentalAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
item-name	Indicates the name of the resource item.

Impact on the System

Under the control of the license, the usage percentage of service resources cannot exceed the threshold defined by the license. Therefore, if a larger license file cannot be applied for or activated, traffic loads cannot cater for the demand of the current operation scenario.

NOTE

This trap is reported only once when the percentage of resources used by the service module reaches or exceeds 90% of the threshold defined by the license.

Possible Causes

The usage percentage of service resources reached or exceeded the threshold defined by the license.

Procedure

- Step 1** Confirm whether the current license file is large enough. If not, apply for a larger license file.
- Step 2** Use the new license file and run the **license active** *license-name* command to activate it.

Step 3 Collect alarm information and configuration information, and then contact technical support personnel.

----End

Related Information

None

3.3.228 ALM-1099702273 License feature is near deadline

Description

GTL/2/NEARDEADLINE:OID [OID] License feature [item-name] is near deadline, remain time is [date] days.

The trap was generated when the system date was approaching the deadline of the service module defined in the license, that is, when the license entered the trial status.

Attribute

Alarm ID	Alarm Severity	Alarm Type
1099702273	Major	environmentalAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
item-name	Indicates the name of the resource item.
date	Indicates the number of remaining days.

Impact on the System

If the new license file is not applied for and activated before the probation period of the existing license file expires, the function items subject to the license will become unavailable and resource items will run as a smaller default value.

NOTE

This trap is reported once a day within the trial period.

Possible Causes

The license was approaching the deadline and soon would become invalid.

Procedure

- Step 1** This trap indicates that the current license file nearly reaches the deadline, and you should apply for the new license file before the deadline.
- Step 2** Use the new license file and run the **license active** *license-name* command to activate it.
- Step 3** Collect alarm information and configuration information, and then contact technical support personnel.

----End

Related Information

None

3.3.229 ALM-1099702274 Current license value is default

Description

GTL/2/DEFAULTVALUE:OID [OID] Current license value is default, the reason is [reason].

The system used the default configuration of the GTL license, when a license file became invalid.

Attribute

Alarm ID	Alarm Severity	Alarm Type
1099702274	Major	environmentalAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
reason	Indicates the cause for default authorization.

Impact on the System

1. Restricted function items in the license will become unavailable.

2. The thresholds of the resource items in the license will be set the default values.

 NOTE

If the GTL License file is invalid, the trap will be reported each time the device restarts or a master/slave main control board switchover is performed.

Possible Causes

The authentication of the license file failed.

Procedure

- Step 1** Confirm whether the license file exists. If not, activate a valid license file.
- Step 2** Confirm whether the license file is valid. If not, replace it with a valid license file.
- Step 3** Collect alarm information and configuration information, and then contact technical support personnel.

----End

Related Information

None

3.3.230 ALM-1099702275 Clear the alarm indicating that resources are nearly exhausted

Description

GTL/2/GTL_NEARUSEDUP_CLEAR: OID [OID] The alarm indicating that resources item [item-name] are nearly exhausted was cleared.

The alarm indicating that the resources available for the service module are running out was cleared.

Attribute

Alarm ID	Alarm Severity	Alarm Type
1099702275	Major	environmentalAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.

Name	Meaning
item-name	Indicates the name of the resource item.

Impact on the System

Services will not be affected.

Possible Causes

The resource usage falls below the threshold.

Procedure

This alarm is informational only, and no action is required.

Related Information

None

3.3.231 ALM-1099702276 Clear the alarm indicating that the license feature is about to expire

Description

GTL/2/GTL_NEARDEADLINE_CLEARED:OID [OID] The alarm indicating that the feature is about to expire was cleared. (FeatureName=[FeatureName])

The alarm indicating that the license was about to expire was cleared.

Attribute

Alarm ID	Alarm Severity	Alarm Type
1099702276	Major	environmentalAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
FeatureName	Indicates the name of the resource item.

Impact on the System

Services will not be affected.

Possible Causes

Cause 1: A valid license file has been loaded, and the license that was about to expire restored to the normal state.

Cause 2: The original license file became invalid.

Procedure

Step 1 Cause 1: This alarm is informational only, and no action is required.

Step 2 Cause 2: Apply for a new valid license file and use the new license file. Run the **license active** *license-name* command to activate the license file.

----End

Related Information

None

3.3.232 ALM-1099702277 Clear the alarm indicating that the default license authorization value is used

Description

GTL/2/GTL_DEFAULTVALUE_CLEARED:OID [OID] The alarm indicating that the system will use the default value if license verification fails was cleared.
(Reason=[Reason])

The alarm indicating that the GTL license values were default settings was cleared.

Attribute

Alarm ID	Alarm Severity	Alarm Type
1099702277	Major	environmentalAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
Reason	Indicates the cause for default authorization.

Impact on the System

None

Possible Causes

A license file was loaded.

Procedure

This alarm is informational only, and no action is required.

Related Information

None

3.3.233 ALM-1099702282 The mismatch between the device ESN and license file

Description

GTL/2/GTL_ESN_MISMATCH:OID [OID] The ESN of slot [slot] mismatched with the license file.

The slot ESN mismatched the GTL license ESN.

Attribute

Alarm ID	Alarm Severity	Alarm Type
1099702282	Major	environmentalAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
slot	ID of the slot

Impact on the System

The GTL license enters the trial period. If a new GTL license is not applied for and activated before the trial period expires, the function items subject to the license will become unavailable and resource items will run under default settings.

Possible Causes

The GTL license ESN mismatched the slot ESN.

Procedure

- Step 1** Run the **license revoke** command to obtain the revoke ticket of the GTL license.
- Step 2** Run the **display esn** command to collect the ESN information.
- Step 3** Apply for a new GTL license by using the revoke ticket and ESN.
- Step 4** Run the **license active** *license-name* command to activate the new GTL license.
- Step 5** Collect alarm information and configuration information, and then contact technical support personnel.

----End

Related Information

None

3.3.234 ALM-1099702283 Clear the alarm indicating that the mismatch between the device ESN and license file

Description

GTL/2/GTL_ESN_MISMATCH_CLEARED:OID [OID] The alarm indicating that the ESN of slot [slot] mismatched with the license file was cleared.

The alarm indicating the mismatch between the slot ESN and GTL license ESN was cleared.

Attribute

Alarm ID	Alarm Severity	Alarm Type
1099702283	Major	environmentalAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
slot	ID of the slot

Impact on the System

None

Possible Causes

A new license was obtained and activated. The slot ESN and GTL license ESN matched again.

Procedure

This trap message is informational only, and no action is required.

Related Information

None

3.3.235 ALM-1099702284 Item is inactive

Description

GTL/2/GTL_ITEM_INACTIVE:OID [OID] Item [item-name] is inactive.

The service module to be controlled by the GTL file was not included in the file but the associated service was successfully configured.

Attribute

Alarm ID	Alarm Severity	Alarm Type
1099702284	Major	environmentAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
item-name	Service module name

Impact on the System

Services controlled by the GTL file will fail.

Possible Causes

The service module to be controlled by the GTL file was not included in the file.

Procedure

Step 1 Apply for an associated GTL file.

Step 2 Run the **license active** *license-name* command to activate the GTL file.

Step 3 Collect alarm information and configuration information, and then contact technical support personnel.

----End

Related Information

None

3.3.236 ALM-1099702285 Clear the alarm indicating that the item is inactive

Description

GTL/2/GTL_ITEM_INACTIVE_CLEARED:OID [OID] The alarm indicating that item [item-name] is inactive was cleared.

The trap generated when the GTL file involving the current service module was inactive was cleared.

Attribute

Alarm ID	Alarm Severity	Alarm Type
1099702285	Major	environmentalAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
item-name	Service module name

Impact on the System

The system will not be affected.

Possible Causes

A GTL file involving the current service module was obtained and activated.

Procedure

This log message is informational only, and no action is required.

Related Information

None

3.3.237 ALM-3276800212 MAC address flapping occurs in a VSI

Description

L2IFPPI/4/MFLPVSIALARM: OID [OID] MAC move detected, VSI-Name=[OCTET], [OCTET].

MAC address flapping occurs in a VSI.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800212	Warning	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
VSI-Name	Indicates a VSI name.
OCTET	Indicates MAC address flapping information.

Impact on the System

Traffic cannot be received correctly.

Possible Causes

- Cause1: The interfaces that form a loop are added to the same VSI.
- Cause2: Cables are connected incorrectly.
- Cause3: No loop prevention protocol such as STP is enabled.
- Cause4: If protocols such as LLDP, LNP, NDP, NTDP, and LACP are enabled on blocked ports, protocol packets are forcibly transmitted through the blocked port. As a result, MAC address flapping occurs on the network connected to the blocked port.

Procedure

Step 1 Connect cables on the interfaces correctly and check whether the alarm persists.

- If so, go to step 2.
- If not, go to step 10.

- Step 2** Check whether the two interfaces that learn the same MAC address can be added to different VSIs according to the networking.
- If so, go to step 3.
 - If not, go to step 4.
- Step 3** Add the two interfaces that learn the same MAC address to different VSIs. Then check whether the alarm persists.
- If so, go to step 4.
 - If not, go to step 10.
- Step 4** Enable a loop prevention protocol such as STP. Check whether the alarm persists.
- If so, go to step 5.
 - If not, go to step 10.
- Step 5** Check whether loops are caused by protocols such as LLDP, LNP, NDP, NTDP, and LACP.
- If so, go to step 6.
 - If not, go to step 9.
- Step 6** Check whether the packets need to be transparently transmitted.
- If so, go to step 8.
 - If not, go to step 7.
- Step 7** Disable the corresponding protocols on the blocked port. Then check whether the alarm persists.
- If so, go to step 9.
 - If not, go to step 10.
- Step 8** Apply a traffic policy that can match the destination MAC address of the protocol packets on the device where MAC address flapping occurs so that source MAC addresses of protocol packets are not learnt. Then check whether the alarm persists.
- If so, go to step 9.
 - If not, go to step 10.
- Step 9** Contact technical support personnel.
- Step 10** End.
- End

Related Information

None

3.3.238 ALM-3276800213 MAC address flapping occurs in a BD

Description

L2IFPPI/4/MFLPBDALARM: OID [OID] MAC move detected, bridge-domain ID=[GAUGE], original-port=[OCTET1], flapping-port 1=[OCTET2], flapping-port 2=[OCTET3], [OCTET4].

MAC address flapping occurs in a BD.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800213	Warning	environmentalAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
GAUGE	Indicates the ID of a BD.
OCTET1	Indicates the number of the interface that learns the MAC address earlier.
OCTET2	Indicates the number of the interface that learns the MAC address later.
OCTET3	Indicates the number of the interface that learns the MAC address later.
OCTET4	Indicates the alarm cause.

Impact on the System

Traffic cannot be received correctly.

Possible Causes

A MAC address in a BD is learned by different interfaces, causing MAC address flapping.

Procedure

Step 1 Perform the following operations to remove loops:

Check information about the two interfaces that learn the same MAC address in the alarm. Shut down one of the two interfaces according to the networking and go to step 2.

Step 2 Check whether the alarm is generated again.

- If so, another loop exists. Shut down one of the two interfaces to eliminate the loop.
- If not, go to step 3.

Step 3 End.
----End

Related Information

None

3.3.239 ALM-3276800214 A loop is detected on the Layer 2 network connected to the interface

Description

LBDT/4/PORTTRAP: OID [OID] Loopback exists on interface([INTEGER1]) [OCTET1] ([OCTET2]), loopback detection status: [INTEGER2], auto loop detection for trap only on VLAN [OCTET3].(Status 1:normal; 2:block; 3:shutdown; 4:trap; 5:nolearn; 6:quitvlan)
A loop is detected on the Layer 2 network connected to the interface.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800214	Warning	Communication alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
INTEGER1	Indicates the interface index.
OCTET1	Indicates the interface name.
OCTET2	An alarm is reported when a loop is detected in a VLAN (not a VLAN in which loops are detected automatically and only alarms are reported). If untagged packets are used to detect the loop, the value of this parameter is Untagged. If tagged packets are used to detect the loop, the value of this parameter is the VLAN ID in the VLAN tag.
INTEGER2	Indicates the loop detection status on the interface.

Name	Meaning
OCTET3	Indicates the list of VLANs where loops are detected automatically. Only alarms are reported.

Impact on the System

After the interface is shut down, all traffic on the interface is interrupted.

After the interface is blocked, all traffic except protocol packets is interrupted.

After nolearn is configured on the interface, the interface does not learn MAC addresses.

After the trap function is configured on the interface, the interface continuously reports traps.

After the quitvlan function is configured on the interface, the interface is deleted from the VLAN where a loop occurs and services of traffic in the VLAN are interrupted.

Possible Causes

An Ethernet loop is detected between the interfaces.

Procedure

A loop occurs on the Layer 2 network connected to the interface.

Related Information

None

3.3.240 ALM-3276800215 A loop is detected on the L2VPN network connected to the interface

Description

LOOPDETECT/4/DetectLoop: OID [OID] The port detected L2VPN loop.
(InterfaceIndex=[INTEGER], InterfaceName=[OCTET], VsiName=[OCTET],
LoopPeVlan=[OCTET], LoopCeVlan=[OCTET])

The device detected a loop on the L2VPN network connected to its interface.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800215	Warning	environmentalAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
InterfaceIndex	Indicates the interface index.
InterfaceName	Indicates the interface name.
VsiName	Indicates the name of the VSI that is bound to the interface.
LoopPeVlan	Indicates the outer ID of the VLAN in which a loop occurs.
LoopCeVlan	Indicates the inner ID of the VLAN in which a loop occurs.

Impact on the System

After the interface is blocked, all the traffic except protocol packets will be blocked.

Possible Causes

- Cause 1: Two interfaces on the CE are connected to the same PE, leading to an L2VPN loop.
- Cause 2: One interface on the CE is dual homed to the same VPLS network, leading to an L2VPN loop.

Procedure

Find the VSI name and VLAN IDs related to the L2VPN loop according to the alarm information. Check whether the loop occurs on the L2VPN network to which the interface connects. If so, eliminate the loop.

Related Information

None

3.3.241 ALM-3276800216 Port detected loopback

Description

MSTP/4/PROLBDETECTGED:OID [OID] The MSTP Process's Port has been set to discarding state because of detecting loopback. (ProcessID=[INTEGER], InstanceID=[INTEGER], PortID1=[INTEGER], PortID2=[INTEGER], PortID3=[INTEGER], PortID4=[INTEGER], PortIDFlag=[INTEGER], IfIndex=[INTEGER], PortState=[INTEGER], PortName=[STRING])

When port detected loopback, block the port and arise trap.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800216	Warning	Communication alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
ProcessID	Indicates the MSTP process ID
InstanceID	Indicates the instance ID.
PortID1	Indicates ID 1 of the port in the MSTP process.
PortID2	Indicates ID 2 of the port in the MSTP process.
PortID3	Indicates ID 3 of the port in the MSTP process.
PortID4	Indicates ID 4 of the port in the MSTP process.
PortIDFlag	Indicates the port flag.
IfIndex	Indicates the port index.
PortState	Indicates the port state.
PortName	Indicates the port name.

Impact on the System

After detecting a port blocked by local loopback, the system considers that a network storm occurs and blocks the local port to prevent the network storm from affecting services of the entire network. Services on the block port will be interrupted.

Possible Causes

When the STP port of the equipment receiving BPDU with the same designated bridge ID and designated port ID as this equipment and port, STP blocks this port and arises this trap for loopback detection will lead loop.

Procedure

- Step 1** Check whether the port where the alarm is generated is configured with local loopback.
- If so, go to Step 4.
 - If not, go to Step 2.
- Step 2** Check whether there is a loop formed by a hub and devices, one of which is connected to the port.
- If so, go to Step 5.
 - If not, go to Step 3.
- Step 3** Collect alarm information and configuration information, and then contact technical support personnel.
- Step 4** Delete the local loopback configuration to solve the problem.
- Step 5** Remove the self-loop network cable from the hub to solve the problem.
- Step 6** End.
- End

Related Information

None

3.3.242 ALM-3276800217 A loop is detected in the network

Description

LDT/4/DetectLoop: OID [OID] The port detected loop. (InterfaceIndex=[integer], InterfaceName=[octet], VlanListLow=[octet], VlanListHigh=[octet])

If the packets that a port sends is returned to the port through the local VLAN, it indicates the packets are looped. A loop may cause a broadcast storm.

A loop is detected.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800217	Warning	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.

Name	Meaning
hwLdtInterfaceIndex	Indicates the index of a port, that is, the index of a physical port at the link layer.
hwLdtInterfaceName	Indicates the name of a port.
hwLdtPortLoopVlanlistLow	Indicates the lower ID of the VLAN that the alarmed port belongs to. The value ranges from 0 to 2047. The value 0 is not used.
hwLdtPortLoopVlanlistHigh	Indicates the higher ID of the VLAN that the alarmed port belongs to. The value ranges from 2048 to 4095. The value 4095 is not used.

Impact on the System

Packets sent from the interface are sent back to the interface through another interface in the same VLAN. This loop may cause broadcast storms in the VLAN.

Possible Causes

The network where the device locates has a loop.

Procedure

Step 1 Run the **display loop-detection** command in the system view or interface view to check information about loop detection on the interface. The following operations are performed according to the **workmode** field:

- If the value of **workmode** is **trap**, the port sends the trap and records logs without processing a detected loop. You need to clear this alarm manually. Run the **display this** command in the interface view to view the VLAN that the port belongs to. Then go to step 2.
- If the value of **workmode** is **block**, the port sends the Trap alarm, records logs, blocks the port, and deletes the MAC address forwarding entry. Go to step 3.
- If the value of **workmode** is **nolearning**, the system sends the Trap alarm, records logs, disables the port from learning MAC addresses, and keeps the normal packet forwarding function of the port. Go to step 3.
- If the value of **workmode** is **shutdown**, the system sends the Trap alarm and records logs. The port is disabled automatically. Go to step 3.
- If the value of **workmode** is **quitvlan**, the system sends traps and records logs, and deletes the interface from the VLAN where a loop occurs. Go to step 3.

Step 2 Remove the loop manually.

Do as follows to remove the loop manually:

- Disconnect the alarmed port manually.
Solution:
 - Remove the connection cable on the port where the loop alarm is generated.
 - Run the **shutdown** command in the interface view to set the port to **down** state.
- Run the **loop-detection mode** command to set the port to a working mode other than the **Trap** mode. Then the system processes the alarm automatically.

Step 3 Wait until the interface recovery time expires, and check whether a clear alarm is received.

(1) If a clear alarm is received, go to step 5.

(2) If not, go to step 4.

Step 4 Contact technical support personnel.

Step 5 End.

----End

Related Information

None

3.3.243 ALM-3276800219 MAC address flapping has occurred

Description

L2IFPPI/4/MFLPVLANALARM: OID [OID] MAC move detected, VLANID=[INTEGER], [OCTET].

MAC address flapping has occurred.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800219	Warning	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
INTEGER	Indicates the VLAN ID.

Name	Meaning
OCTET	Indicates the flapping MAC address and interfaces between which the MAC address flaps.

Impact on the System

Traffic cannot be received normally.

Possible Causes

1:

The interfaces where loops occur are added to the same VLAN.

2:

Cables are connected incorrectly.

3:

STP is enabled to remove loops on the network.

Procedure

- Step 1** Check that cables are connected correctly. Then check whether the alarm is still reported.
- If yes, go to step 2.
 - If not, go to step 6.
- Step 2** Check whether the two interfaces that learn the same MAC address can be added to different VLANs according to the networking.
- If yes, go to step 3.
 - If not, go to step 4.
- Step 3** Modify the configuration and add the two interfaces that learn the same MAC address to different VLANs. Then check whether the alarm is still reported.
- If yes, go to step 4.
 - If not, go to step 6.
- Step 4** Enable STP. Then check whether the alarm is still reported.
- If yes, go to step 5.
 - If not, go to step 6.
- Step 5** Contact technical support personnel.
- Step 6** End.
- End

Related Information

None

3.3.244 ALM-3276800305 Indicates that the CSS port state has changed to down

Description

CSSM/3/CSSLINKDOWN: OID [OID] [INTEGER1]/[INTEGER2] CSS port [INTEGER3] down.

The CSS port goes Down.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800305	Minor	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
INTEGER1	Indicates the chassis ID.
INTEGER2	Indicates the slot ID.
INTEGER3	Indicates the port number.

Impact on the System

Bandwidth between the CSS devices is reduced or the CSS breaks up.

Possible Causes

- 1: The CSS cable is removed or loose.
- 2: The CSS cable is faulty.

Procedure

Step 1 Check whether the cable is connected securely to the CSS port.

- If not, connect the CSS cable to the port securely.
- If so, go to step 2.

Step 2 Check whether the indicator on the CSS card is on.

- If not, replace the cable.
- If so, go to step 3.

Step 3 Check whether a clear alarm is generated.

- If so, no action is required.
- If not, collect alarm information and configuration information, and then contact technical support personnel.

----End

Related Information

None

3.3.245 ALM-3276800474 The number of DHCPv6 Request messages that were discarded on an interface because they did not match the binding entries exceeded the threshold

Description

DHCP/1/DHCPV6REQUESTTRAP:OID [OID] The number of the discarded DHCPv6 request packets that do not match the binding table exceeds the threshold on the interface. (Interface=[OCTET], VlanID=[INTEGER], BdID=[INTEGER], LastDroppedSourceMac=[OCTET], DiscardedNumber=[INTEGER])

The number of DHCPv6 Request messages that were discarded on an interface because they did not match the binding entries exceeded the threshold.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800474	Warning	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
Interface	Interface name.
VlanID	VLAN ID.
BdID	Indicates the BD ID.
LastDroppedSourceMac	Source MAC address of the last discarded message.

Name	Meaning
DiscardedNumber	Number of discarded messages.

Impact on the System

Invalid DHCPv6 Request messages are discarded.

Possible Causes

Attacks from bogus DHCPv6 users were received.

Procedure

1. Run the **display dhcpv6 snooping user-bind** command to check information about DHCPv6 snooping binding entries on the interface and determine the interface or VLAN from which the user goes online based on the source MAC address of the last discarded message.
2. Obtain the DHCPv6 Request messages received on the interface or in the VLAN using the port mirroring method.
 - If a user connected to the interface sends a large number of DHCPv6 Request messages that do not match the binding entries, the user is an unauthorized user and the sent messages are attack messages. The device discards the attack messages. Check the attack source based on the user's IPv6 address or MAC address.
 - If users connected to the interface do not send a large number of DHCPv6 Request messages that do not match the binding entries, the messages sent by the users are not attack messages. To ensure that the users pass the check, cancel the **dhcp snooping check dhcp-request enable** command configuration on the interface.

Related Information

None

3.3.246 ALM-3276800475 The number of the discarded DHCP packets in which the CHADDR field is inconsistent with the source MAC address exceeds the threshold on the interface

Description

DHCP/1/REQMACTRAP:OID [OID] The number of the discarded DHCP packets in which the CHADDR field is inconsistent with the source MAC address exceeds the threshold on the interface. (IfIndex=[INTEGER], VlanIndex=[INTEGER], Interface=[OCTET], VlanID=[INTEGER], BdlID=[INTEGER], DiscardedNumber=[INTEGER])

The number of discarded DHCP packets in which the CHADDR field and the source MAC address mismatched exceeded the threshold on the interface.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800475	Warning	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
IfIndex	Indicates the interface index.
VlanIndex	Indicates the VLAN index.
Interface	Indicates the interface name.
VlanID	Indicates the VLAN ID.
BdID	Indicates the BD ID.
DiscardedNumber	Indicates the number of discarded packets.

Impact on the System

Invalid DHCP packets are discarded.

Possible Causes

The device considers DHCP packets in which the CHADDR field does not match the source MAC address as invalid DHCP packets.

Procedure

- Configure port mirroring to obtain DHCP packets received by the interface. Check whether DHCP packets in which the CHADDR field does not match the source MAC address are attack packets.
 - If a user connected to the interface sends a large number of DHCP packets in which the CHADDR field does not match the source MAC address, the user is an unauthorized user and the DHCP packets are attack packets. The device discards the attack packets. Check the attack source based on the source address.
 - If users connected to the interface do not send a large number of DHCP packets in which the CHADDR field does not match the source MAC address, DHCP packets sent by the users are not attack packets. To ensure that the users pass the check, cancel the **dhcp snooping check dhcp-chaddr enable** command configuration on the interface.

Related Information

None

3.3.247 ALM-3276800476 The number of the discarded DHCP request packets that do not match the binding table exceeds the threshold on the interface

Description

DHCP/1/REQUESTTRAP:OID [OID] The number of the discarded DHCP request packets that do not match the binding table exceeds the threshold on the interface. (IfIndex=[INTEGER], VlanIndex=[INTEGER], Interface=[OCTET], VlanID=[INTEGER], BdID=[INTEGER], DiscardedNumber=[INTEGER])

The number of DHCP Request packets discarded on the interface because they do not match the binding table exceeded the threshold.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800476	Warning	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
IfIndex	Indicates the interface index.
VlanIndex	Indicates the VLAN index.
Interface	Indicates the interface name.
VlanID	Indicates the VLAN ID.
BdID	Indicates the BD ID.
DiscardedNumber	Indicates the number of discarded packets.

Impact on the System

Invalid DHCP packets are discarded.

Possible Causes

DHCP attacks occurred.

Procedure

1. Run the **display dhcp snooping user-bind** command to check DHCP snooping binding entries on the interface to determine users' IP addresses and MAC addresses.
2. Configure port mirroring to obtain DHCP packets received by the interface. Check users' IP addresses and MAC addresses in DHCP Request packets that do not match the binding table.
 - If a user connected to the interface sends a large number of DHCP Request packets that do not match the binding table, the user is an unauthorized user and the DHCP Request packets are attack packets. The device discards the attack packets. Check the attack source based on the user's IP address or MAC address.
 - If users connected to the interface do not send a large number of DHCP Request packets that do not match the binding table, DHCP packets sent by the users are not attack packets. To ensure that the users pass the check, cancel the **dhcp snooping check dhcp-request enable** command configuration on the interface.

Related Information

None

3.3.248 ALM-3276800477 The number of ND packets that were discarded on an interface because they did not match the binding entries exceeded the threshold

Description

DHCP/1/NDBINDCHECKTRAP:OID [OID] The number of the discarded ND packets that do not match the binding table exceeds the threshold on the interface. (Interface=[OCTET], VlanID=[INTEGER], LastDroppedSourceMac=[OCTET], DiscardedNumber=[INTEGER])

The number of ND packets that were discarded on an interface because they did not match the binding entries exceeded the threshold.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800477	Critical	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.

Name	Meaning
Interface	Interface name.
VlanID	VLAN ID.
LastDroppedSourceMac	Source MAC address of the last discarded packet.
DiscardedNumber	Number of discarded packets.

Impact on the System

Invalid ND packets are discarded.

Possible Causes

Attacks from bogus ND users were received.

Procedure

1. Run the **display nd snooping user-bind** command to check information about ND snooping binding entries on the interface and determine the interface or VLAN from which the user goes online based on the source MAC address of the last discarded packet.
2. Obtain the ND packets received on the interface or in the VLAN using the port mirroring method.
 - If a user connected to the interface sends a large number of ND packets that do not match the binding entries, the user is an unauthorized user and the sent packets are attack packets. The device discards the attack packets. Check the attack source based on the user's IPv6 address or MAC address.
 - If a user connected to the interface does not send a large number of ND packets that do not match the binding entries, the packets sent by the user are not attack packets. To ensure that the users pass the check, cancel the **nd snooping check { na | ns | rs } enable** command configuration on the interface.

Related Information

None

3.3.249 ALM-3276800478 The number of packets in a VLAN discarded by IPSG

Description

SECE/4/IPSG_VLANDROP_ALARM:OID [OID] The packet dropped by IPSG exceeds the alarm threshold. (DroppedNum=[INTEGER], Threshold=[INTEGER], VLAN=[INTEGER], PacketInfo=[OCTET])

The number of packets in a VLAN discarded by IPSG exceeded the alarm threshold.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800478	Warning	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
DroppedNum	Indicates the number of discarded packets.
Threshold	Indicates the alarm threshold.
VLAN	Indicates the VLAN ID of discarded packets.
PacketInfo	Indicates the VLAN ID, source MAC address, and source IP address of packets.

Impact on the System

If this alarm is generated, the device may be attacked. If the attack traffic volume is heavy, the device is busy processing attack packets. As a result, services of authorized users are interrupted.

Possible Causes

The number of packets discarded by IPSG exceeded the alarm threshold. This threshold can be configured using the **ip source check user-bind alarm threshold** command. The default alarm threshold is 100.

Procedure

1. Find the VLAN where attacks occur according to **VLAN** in the alarm message.
2. Run the **display dhcp snooping user-bind** command to check whether users who are not in the DHCP snooping binding table range are connected.
3. If new users are connected, run related DHCP snooping commands to generate the DHCP snooping binding table.

Related Information

None

3.3.250 ALM-3276800479 The number of the discarded DHCP reply packets on the untrusted interface exceeds the threshold

Description

DHCP/1/REPLYTRAP:OID [OID] The number of the discarded DHCP reply packets on the untrusted interface exceeds the threshold. (IfIndex=[INTEGER], VlanIndex=[INTEGER], Interface=[OCTET], VlanID=[INTEGER], BdID=[INTEGER], DiscardedNumber=[INTEGER])

The number of DHCP Reply packets discarded on the untrusted interface exceeded the threshold.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800479	Warning	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
IfIndex	Indicates the interface index.
VlanIndex	Indicates the VLAN index.
Interface	Indicates the interface name.
VlanID	Indicates the VLAN ID.
BdID	Indicates the BD ID.
DiscardedNumber	Indicates the number of discarded packets.

Impact on the System

Invalid DHCP packets are discarded.

Possible Causes

Bogus DHCP server attacks occurred.

Procedure

1. Capture packets on the interface to check whether a bogus DHCP server attack occurs on this interface.
 - Check whether the DHCP server address in the received DHCP Reply packet is the specified server address. If not, the DHCP server is a bogus server. Because the invalid DHCP packets have been discarded, no action is required.
 - If the DHCP server is a valid server and needs to be used, run the **dhcp snooping trusted** command on the interface to configure it as a trusted interface.

Related Information

None

3.3.251 ALM-3276800480 The number of packets discarded by DAI exceeds the alarm threshold

Description

SECE/4/DAI_BDDROP_ALARM: OID [oid] The packet dropped by DAI exceeds the alarm threshold. (DroppedNum=[INTEGER], Threshold=[INTEGER], BD=[INTEGER], PacketInfo=[OCTET]).

The number of packets discarded by Dynamic ARP Inspection (DAI) in a BD exceeds the alarm threshold.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800480	Warning	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
DroppedNum	Indicates the number of discarded packets.
Threshold	Indicates the alarm threshold.
BD	Indicates the ID of the BD where the DAI alarm function is configured.

Name	Meaning
PacketInfo	Indicates the interface, VLAN, source MAC address, and source IP address of the packets.

Impact on the System

If this alarm is generated, the device may be attacked. If the attack traffic volume is heavy, the device is busy processing attack packets. As a result, services of authorized users are interrupted.

Possible Causes

The number of packets discarded by DAI in a BD exceeds the alarm threshold. By default, the alarm threshold for ARP packets discarded by DAI is 100.

Procedure

- If user services are not affected, the alarm does not need to be handled.
- If user services are interrupted, perform the following operations:
 - a. Run the **display dhcp snooping user-bind** { { **interface** *interface-type interface-number* | **ip-address** *ip-address* | **mac-address** *mac-address* | **vlan** *vlan-id* | **bridge-domain** *bd-id* } * | **all** } [**verbose**] command to check the dynamic binding entries to see whether they are correct.
 - b. Find out the interface and user host that initiate the attack. Check whether the host is attacked. If not, the host belongs to the attacker. Take measures to defend against the attack, for example, disconnect the attacker's host.
 - c. Collect alarm and configuration information, and contact technical support.

Related Information

None

3.3.252 ALM-3276800307 Interface input flow bandwidth usage exceeded the trap threshold

Description

IFNET/4/INBWRATEEXCEED: OID [OID] Interface input flow bandwidth usage exceeded the trap threshold. (Interface=[INTEGER], BandWidthUsage=[INTEGER], TrapThreshold=[INTEGER], InterfaceName=[STRING])

The trap was generated when the percentage of the rate of received traffic to the total bandwidth on an interface was greater than the threshold.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800307	Warning	Quality of service alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
Interface	Indicates the interface index.
BandWidthUsage	Indicates bandwidth usage.
TrapThreshold	Indicates the trap threshold of bandwidth usage.
InterfaceName	Indicates the interface name.

Impact on the System

When traffic rate is approximate to the maximum interface bandwidth, service packets may be dropped.

Possible Causes

The rate of traffic received by the interface was too large.

Procedure

- Step 1

Run the **display this interface** command on the interface to check whether the traffic threshold is too low. The threshold range is specified by users according to actual services.

• If so, go to Step 2.

• If not, go to Step 3.
- Step 2

Run the **trap-threshold output-rate** *threshold_value* command to reset the threshold and then check whether the alarm is cleared.

• If so, go to Step 7.

• If not, go to Step 3.
- Step 3

Run the **display this interface** command in the interface view to check the number and types of packets on the interface. Determine whether the packet sending and receiving is abnormal due to a failure such as loop.

• If so, go to Step 4.

• If not, go to Step 5.

Step 4 Find out the abnormal packets and eliminate the impact of abnormal packets. Check whether the alarm is cleared.

- If so, go to Step 7.
- If not, go to Step 5.

Step 5 Expand capacity in any of the following ways:

- Configure an Eth-Trunk to load balance traffic.
- Migrate some services to idle devices.
- Use the link with higher bandwidth to transmit service packets.

After the operation, check whether the alarm is cleared.

- If so, go to Step 7.
- If not, go to Step 6.

Step 6 Collect trap messages, log messages, and configurations, and then contact the technical support personnel.

Step 7 End.

----End

Related Information

None

3.3.253 ALM-3276800308 Interface output flow bandwidth usage exceeded the trap threshold

Description

IFNET/4/OUTBWRATEEXCEED: OID [OID] Interface output flow bandwidth usage exceeded the trap threshold. (Interface=[INTEGER], BandWidthUsage=[INTEGER], TrapThreshold=[INTEGER], InterfaceName=[STRING])

The trap was generated when the percentage of the rate of sent traffic to the total bandwidth on an interface was greater than the threshold.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800308	Warning	Quality of service alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.

Name	Meaning
Interface	Indicates the interface index.
BandWidthUsage	Indicates bandwidth usage.
TrapThreshold	Indicates the trap threshold of bandwidth usage.
InterfaceName	Indicates the interface name.

Impact on the System

When traffic rate is approximate to the maximum interface bandwidth, service packets may be dropped.

Possible Causes

The rate of traffic sent by the interface was too large.

Procedure

- Step 1** Run the **display this interface** command on the interface to check whether the traffic threshold is too low. The threshold range is specified by users according to actual services.
- If so, go to Step 2.
 - If not, go to Step 3.
- Step 2** Run the **trap-threshold output-rate *threshold_value*** command to reset the threshold and then check whether the alarm is cleared.
- If so, go to Step 7.
 - If not, go to Step 3.
- Step 3** Run the **display this interface** command in the interface view to check the number and types of packets on the interface. Determine whether the packet sending and receiving is abnormal due to a failure such as loop.
- If so, go to Step 4.
 - If not, go to Step 5.
- Step 4** Find out the abnormal packets and eliminate the impact of abnormal packets. Check whether the alarm is cleared.
- If so, go to Step 7.
 - If not, go to Step 5.
- Step 5** Expand capacity in any of the following ways:
- Configure an Eth-Trunk to load balance traffic.
 - Migrate some services to idle devices.
 - Use the link with higher bandwidth to transmit service packets.

After the operation, check whether the alarm is cleared.

- If so, go to Step 7.
- If not, go to Step 6.

Step 6 Collect trap messages, log messages, and configurations, and then contact the technical support personnel.

Step 7 End.

----End

Related Information

None

3.3.254 ALM-4289601646 Indicates that the NETCONF database is abnormal

Description

ENTITYTRAP/1/NETCONFDBABNORMAL: OID [oid] The NETCONF database is abnormal.

The NETCONF database is abnormal.

Attribute

AlarmID	Alarm OID	Alarm Severity	Alarm Type
4289601646	1.3.6.1.4.1.2011.5.25.2 19.2.11.11	Critical	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.

Impact on the System

The device configuration information cannot be delivered, causing service exceptions.

Possible Causes

An internal processing error occurs on the device.

Procedure

Step 1 On the controller, deliver the backup NETCONF database information again.

Step 2 On the controller, deliver a command to restart the device.

----End

3.3.255 ALM-1707675687 The status of the terminal is abnormal.

Description

SECE/4/TERMINAL_STATUS_ABNORMAL:OID [OID] The status of the terminal is abnormal. (Interface=[OCTET], SourceMAC=[OCTET], TerminalType=[OCTET], IPAddress=[OCTET])

The NETCONF database is abnormal.

Attribute

AlarmID	Alarm OID	Alarm Severity	Alarm Type
1707675687	1.3.6.1.4.1.2011.5.25.16 5.2.2.15.1	Warning	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
Interface	Indicates the interface name.
SourceMAC	Indicates the source MAC address of terminal.
TerminalType	Indicates the terminal type.
IPAddress	Indicates the ip address of terminal.

Impact on the System

- If a service uses the static CR-LSP as the tunnel, traffic is interrupted. If a backup path is configured for the static CR-LSP, traffic is switched to the backup path. If no service uses the static CR-LSP, the static CR-LSP is not affected.

- If the PVC status changes to inactive, the PVC channel becomes unavailable and the MAP entries corresponding to the PVC are deleted. As a result, traffic forwarding fails.
- Policies cannot be delivered to the Front End, and all services cannot be processed.

Possible Causes

Cause 1:

The terminal is spoofed.

Cause 2:

The terminal is infected with viruses or is installed with Trojan horses.

Cause 3:

The terminal is abnormal, for example, the system breaks down or the camera is blocked.

Cause 4:

The new type of UEs and the system does not support this terminal abnormal status identification and reporting.

Procedure

- Step 1** Check the validity of the alarm terminal and bring the unauthorized terminal offline.
- Step 2** If the terminal is valid, check the working status of the terminal and avoid the terminal is crashing.
- Step 3** New types of UEs want to support this feature and the exception detection software needs to be upgraded.
- End

Related Information

None

3.3.256 ALM-1707675688 Static MAC address flapping occurs

Description

L2IFPPI/4/PORTSECSTATICFLP: OID [OID] Interface received a packet with flapping static MAC. (MACAddr=[OPAQUE], VLAN=[GAUGE], VsiName=[OCTET], IfIndex=[INTEGER], InterfaceName=[OCTET])

The source MAC address in the packet received by an interface already exists in the static MAC table of another interface.

Attribute

AlarmID	Alarm OID	Alarm Severity	Alarm Type
1707675688	1.3.6.1.4.1.2011.5.25.315.3.9	Warning	Quality of service alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm
MACAddr	Indicates the MAC address
VLAN	Indicates the VLAN ID
VsiName	Indicates the name of a VSI
IfIndex	Indicates the interface index
InterfaceName	Indicates the interface name

Impact on the System

The source MAC address in the packet received by an interface already exists in the static MAC table of another interface. Therefore, the interface will discard this packet.

Possible Causes

The source MAC address of the packet received by an interface enabled with port security exists in a static MAC address entry on another interface.

Procedure

1. Check whether the interface needs to process the packet.
 - If so, go to [step 2](#).
 - If not, go to [step 3](#).
2. Run the **display mac-address [vlan vlan-id | interface-type interface-number] *** command to search for the corresponding interface based on the MAC address of the packet, and run the **undo mac-address [interface-type interface-number | vlan vlan-id] *** command on the interface to delete the existing MAC address entry.
3. End.

Clearing

The alarm needs to be cleared manually.

3.3.257 ALM-3276800485 The packet dropped by DAI exceeds the alarm threshold

Description

SECE/4/ DAI_VLANDROP_ALARM: OID [oid] The packet dropped by DAI exceeds the alarm threshold. (DroppedNum=[INTEGER], Threshold=[INTEGER], VLAN=[INTEGER], PacketInfo=[OCTET])

The number of packets discarded by Dynamic ARP Inspection (DAI) in a VLAN exceeds the alarm threshold.

Attribute

AlarmID	Alarm OID	Alarm Severity	Alarm Type
3276800485	1.3.6.1.4.1.2011.5.25.16 5.2.2.2.17	Warning	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
DroppedNum	Indicates the number of discarded packets.
Threshold	Indicates the alarm threshold.
VLAN	Indicates the ID of the VLAN where the DAI alarm function is configured.
Interface	Indicates the interface, VLAN, source MAC address, and source IP address of the packets.

Impact on the System

If this alarm is generated, the device may be attacked. If the attack traffic volume is heavy, the device is busy processing attack packets. As a result, services of authorized users are interrupted.

Possible Causes

The number of packets discarded by DAI in a VLAN exceeds the alarm threshold. By default, the alarm threshold for ARP packets discarded by DAI is 100.

Procedure

- If user services are not affected, the alarm does not need to be handled.
- If user services are interrupted, perform the following operations:
 - a. Run the **display dhcp static user-bind** { { **interface** *interface-type interface-number* | **ip-address** *ip-address* | **mac-address** *mac-address* | **vlan** *vlan-id* } * | **all** } [**verbose**] or **display dhcpv6 static user-bind** { { **interface** *interface-type interface-number* | **ipv6-address** { *ipv6-address* | **all** } | **mac-address** *mac-address* | **vlan** *vlan-id* } * | **all** } [**verbose**] command to check the static binding entries, and run the **display dhcp snooping user-bind** { { **interface** *interface-type interface-number* | **ip-address** *ip-address* | **mac-address** *mac-address* | **vlan** *vlan-id* | **bridge-domain** *bd-id* } * | **all** } [**verbose**] command to check the dynamic binding entries to see whether they are correct.
 - b. Find out the interface and user host that initiate the attack. Check whether the host is attacked. If not, the host belongs to the attacker. Take measures to defend against the attack, for example, disconnect the attacker's host.
 - c. Collect log and configuration information and contact technical support.

Clearing

The alarm needs to be cleared manually.

3.3.258 ALM-3276800482 The Number of Flow Entry Resources Occupied by IFIT on a Device Exceeds the Threshold

Description

IFIT/4/SIPFPM_GLOBAL_STREAM_EXCEED: OID [OID] The sipfpm global stream resource exceed the threshold. (Used=[INTEGER], Total=[INTEGER], Threshold=[INTEGER])

The number of flow entry resources occupied by IFIT on a device exceeds 90% of the total number of flow entry resources on the device.

Attribute

Alarm ID	Alarm OID	Alarm Severity	Alarm Type
3276800482	1.3.6.1.4.1.2011.5.2 5.316.3.14	Info	Service quality alarm

Parameters

Name	Meaning
OID	Indicates the ID of the MIB object.

Name	Meaning
Used	Indicates the number of flow entries that have been used on the device.
Total	Indicates the total number of flow entries on the device.
Threshold	Indicates the alarm threshold.

Impact on the System

An IFIT measurement flow or other services that use flow entries cannot be configured.

Possible Causes

The number of flow entry resources occupied by IFIT on a device exceeds the upper threshold.

Procedure

Check the IFIT configuration. You can modify the configuration to delete the traffic flows that do not need to be matched to reduce the number of occupied streams.

Related Information

None

3.3.259 ALM-3276800481 The Number of Flow Entry Resources Occupied by IFIT on a Card Exceeds the Threshold

Description

IFIT/4/SIPFPM_BOARD_STREAM_EXCEED: OID [OID] The sipfpm stream resource on the slot exceed the threshold. (Slot=[OCTET], Used=[INTEGER], Total=[INTEGER], Threshold=[INTEGER])

The number of flow entry resources occupied by IFIT on a single carddevice exceeds 90% of the total number of flow entry resources on the carddevice.

Attribute

Alarm ID	Alarm OID	Alarm Severity	Alarm Type
3276800481	1.3.6.1.4.1.2011.5.2 5.316.3.16	Info	Service quality alarm

Parameters

Name	Meaning
OID	MIB object ID of the alarm.
Slot	Indicates the slot ID of the carddevice.
Used	Indicates the number of flow entries that have been used on the carddevice.
Total	Indicates the total number of flow entries on the carddevice.
Threshold	Indicates the alarm threshold.

Impact on the System

An IFIT measurement flow or other services that use flow entries cannot be configured on the carddevice.

Possible Causes

Services that use flow entries on the carddevice, such as IFIT and NetStream, occupy a large number of resources.

Procedure

Check the IFIT configuration. You can modify the configuration to delete the traffic flows that do not need to be matched to reduce the number of occupied streams.

Related Information

None

3.3.260 ALM-3276800483 The DSCP Value of Packets Matching a Measurement Flow on a Card Conflicts with the IFIT Color Bit

Description

IFIT/4/SIPFPM_BOARD_PKT_DSCP_CONFLICT: OID [OID] The dscp value of the packets matching the sipfpm measurement flow on the card conflicts with the configured sipfpm color-bit. (Slot=[OCTET], IfIndex=[INTEGER], Direction=[OCTET], SrcIp=[OCTET], DstIp=[OCTET], Protocol=[INTEGER], SrcPort=[INTEGER], DstPort=[INTEGER], PktDscp=[INTEGER], CfgDscp=[INTEGER])

The DSCP value of the packets matching a measurement flow and received by an interface is not 0, and conflicts with the IFIT color bit configured on the device.

Attribute

Alarm ID	Alarm OID	Alarm Severity	Alarm Type
3276800483	1.3.6.1.4.1.2011.5.25.316.3.18	Info	Processing error alarm

Parameters

Name	Meaning
OID	Indicates the ID of the MIB object.
Slot	Indicates the slot ID of the carddevice that receives packets matching a measurement flow.
IfIndex	Indicates the index of the interface that receives the measurement flow.
Direction	Indicates the measurement direction of the measurement flow.
SrcIp	Indicates the source IP address of the measurement flow.
DstIp	Indicates the destination IP address of the measurement flow.
Protocol	Indicates the protocol number of the measurement flow.
SrcPort	Indicates the source port number of the measurement flow.
DstPort	Indicates the destination port number of the measurement flow.
PktDscp	Indicates the DSCP value of the packets matching the measurement flow.
CfgDscp	Indicates the configured DSCP value.

Impact on the System

Other services that use DSCP values to provide differentiated services on the network are abnormal.

Possible Causes

In network planning, services that use the DSCP field to provide differentiated services conflict with each other.

Procedure

Check the configuration of the entire network to find out whether the DSCP field is used.

Related Information

None

3.3.261 ALM-3276800484 The error information of the command config

Description

The error information of the command config.

Attribute

AlarmID	Alarm OID	Alarm Severity	Alarm Type
3276800483	-	Major	processingErrorAlarm

Parameters

None.

Impact on the System

None.

Possible Causes

See the information returned by the LSW.

Procedure

See the information returned by the LSW.

Related Information

None

3.3.262 ALM-3276800238 The remote-unit firmware upgrade failed

Description

The remote-unit firmware upgrade failed. (RemoteUnitEsn=[RemoteUnitEsn], InterfaceName=[InterfaceName], Firmware=[Firmware], Reason=[Reason])

An RU fails to be upgraded.

Attribute

AlarmID	Alarm OID	Alarm Severity	Alarm Type
3276800238	1.3.6.1.4.1.2011.5.25.667.2.19	Major	Equipment alarm

Parameters

Name	Meaning
RemoteUnitEsn	ESN of the RU.
InterfaceName	Interconnection port.
Firmware	Firmware type. The value can be APP, PoE, or BIOS.
Reason	Failure cause.

Impact on the System

This alarm is generated when the central switch fails to upgrade an RU. This alarm needs to be manually cleared.

Possible Causes

Cause 1: UpgradeTimeOut: The RU upgrade timed out.

Cause 2: upgrade is break: The upgrade is interrupted. In most cases, this issue occurs if the RU is reset during the upgrade.

Cause 3: no signature: The newly upgraded firmware does not have a signature.

Procedure

1. If the Reason field in the alarm information is UpgradeTimeOut, check whether the communication between the central switch and the RU is normal.
2. If the Reason field in the alarm information is upgrade is break, no special processing is required. The RU will be upgraded again.
3. If the Reason field in the alarm information is no signature, the signature of the firmware patch is incorrect. In this case, contact the firmware patch provider to check whether the signature of the patch is correct.

3.3.263 ALM-4286849027 The number of incoming packets discarded due to congestion on an interface of a remote unit exceeds the threshold

Description

RUMNG/4/RUPTINDISCARDEXCEED:OID [oid] Remote unit interface input discard exceed the trap threshold. (RemoteUnitEsn=[OCTET], InterfaceName=[OCTET], Statistics=[COUNTER64], TrapThreshold=[ULONG], TrapInterval=[ULONG](s))

The number of incoming packets discarded due to congestion on an interface of a remote unit exceeds the alarm threshold. The current threshold is 600 and the interval is 1 minute.

Attribute

AlarmID	Alarm OID	Alarm Severity	Alarm Type
4286849027	1.3.6.1.4.1.2011.5.25.667.2.5	Warning	Quality of service alarm

Parameters

Name	Meaning
oid	Indicates the MIB object ID of the alarm.
RemoteUnitEsn	Indicates the ESN of the remote unit.
InterfaceName	Indicates the name of the interconnection interface.
Statistics	Indicates the statistics in the packet loss period.
TrapThreshold	Indicates the packet loss alarm threshold. The value is fixed at 600.
TrapInterval	Indicates the alarm interval. The value is fixed at 60s.

Impact on the System

If this alarm is generated, severe network congestion occurs on the network. If the fault is not rectified in time, network congestion will cause more packet loss, which will affect the normal running of services.

Possible Causes

The number of incoming packets discarded due to congestion on an interface exceeds the threshold.

Procedure

Collect alarm and configuration information, and contact technical support personnel.

3.3.264 ALM-4286849028 The number of outgoing packets discarded due to congestion on an interface of a remote unit exceeds the threshold

Description

RUMNG/4/RUPORTOUTDISCARDEXCEED:OID [oid] Remote unit interface output discard exceed the trap threshold. (RemoteUnitEsn=[OCTET], InterfaceName=[OCTET], Statistics=[COUNTER64], TrapThreshold=[ULONG], TrapInterval=[ULONG](s))

The number of outgoing packets discarded due to congestion on an interface of a remote unit exceeds the alarm threshold. The current threshold is 600 and the interval is 1 minute.

Attribute

AlarmID	Alarm OID	Alarm Severity	Alarm Type
4286849028	1.3.6.1.4.1.2011.5.25.667.2.7	Warning	Quality of service alarm

Parameters

Name	Meaning
oid	Indicates the MIB object ID of the alarm.
RemoteUnitEsn	Indicates the ESN of the remote unit.
InterfaceName	Indicates the name of the interconnection interface.
Statistics	Indicates the statistics in the packet loss period.
TrapThreshold	Indicates the packet loss alarm threshold. The value is fixed at 600.

Name	Meaning
TrapInterval	Indicates the alarm interval. The value is fixed at 60s.

Impact on the System

If this alarm is generated, severe network congestion occurs on the network. If the fault is not rectified in time, network congestion will cause more packet loss, which will affect the normal running of services.

Possible Causes

The number of outgoing packets discarded due to congestion on an interface exceeds the threshold.

Procedure

Collect alarm and configuration information, and contact technical support personnel.

3.3.265 ALM-4286849029 The number of CRC error packets on an interface of a remote unit exceeds the threshold within a specified period of time

Description

RUMNG/2/RUPOTRCRCERRORRISING:OID [oid] Remote unit CRC error is rising. (RemoteUnitEsn=[OCTET], InterfaceName=[OCTET], CrcErrorStatistics=[COUNTER64], CrcErrorThreshold=[INTEGER], CrcErrorInterval=[INTEGER](s))

The number of CRC error packets on an interface of a remote unit exceeds the alarm threshold within a specified period of time. The current threshold is 20 and the period is 1 minute.

Attribute

AlarmID	Alarm OID	Alarm Severity	Alarm Type
4286849029	1.3.6.1.4.1.2011.5.25.667.2.9	Critical	Quality of service alarm

Parameters

Name	Meaning
oid	Indicates the MIB object ID of the alarm.
RemoteUnitEsn	Indicates the ESN of the remote unit.
InterfaceName	Indicates the name of the interconnection interface.
CrcErrorStatistics	Indicates the statistics in a CRC period.
CrcErrorThreshold	Indicates the CRC alarm threshold. The value is fixed at 20.
CrcErrorInterval	Indicates the alarm interval. The value is fixed at 60s.

Impact on the System

Some service data on the port is discarded.

Possible Causes

- Cause 1: The optical module is faulty.
- Cause 2: The fiber is faulty.

Procedure

1. Replace the optical module and check whether the alarm is cleared.
 - If so, the alarm handling ends.
 - If not, go to step 2.
2. Replace the optical fiber and check whether the alarm is cleared.
 - If so, the alarm handling ends.
 - If not, collect alarm and configuration information and contact technical support personnel.

3.3.266 ALM-4286849030 The remote-unit is online

Description

RUMNG/4/RUONLINE:OID [oid] The remote-unit is online.
(RemoteUnitEsn=[OCTET], ConnectInterface=[OCTET])

The remote-unit is online.

Attribute

AlarmID	Alarm OID	Alarm Severity	Alarm Type
4286849030	1.3.6.1.4.1.2011.5.25.667.2.23	Warning	Quality of service alarm

Parameters

Name	Meaning
oid	Indicates the MIB object ID of the alarm.
ConnectInterface	Interconnection port.
RemoteUnitEsn	Indicates the ESN of the remote unit.

Impact on the System

The remote unit goes online normally.

Possible Causes

The remote-unit is online normally.

Procedure

This alarm is informational only, and no action is required.

3.3.267 ALM-4286849031 The remote-unit is offline

Description

RUMNG/4/RUOFFLINE:OID [oid] The remote-unit is offline.
(RemoteUnitEsn=[OCTET], ConnectInterface=[OCTET], Reason=[OCTET])
The remote-unit is offline.

Attribute

AlarmID	Alarm OID	Alarm Severity	Alarm Type
4286849031	1.3.6.1.4.1.2011.5.25.667.2.25	Warning	Quality of service alarm

Parameters

Name	Meaning
oid	Indicates the MIB object ID of the alarm.
ConnectInterface	Interconnection port.
RemoteUnitEsn	Indicates the ESN of the remote unit.
Reason	Indicates the logout reason.

Impact on the System

The remote unit goes offline.

Possible Causes

- Cause1: Unkown.
- Cause2: No heartbeat
- Cause3: Port down.
- Cause4: One port is connected to multiple remote-units
- Cause5: Manual restart.
- Cause6: Upgrade restart.

Procedure

- Analyze the cause based on the restart scenario and logs.
- Check whether the line is faulty.
- Check the cause of the port down.
- Check whether one port is connected to multiple asteroids.
- No action is required.
- No action is required.

3.3.268 ALM-4286849032 The authentication to the remote unit failed

Description

RUMNG/2/RUAUTHFAIL:OID [oid] The authentication to the remote unit failed.
(RemoteUnitEsn=[OCTET])

The central switch fails to authenticate the remote module.

Attribute

AlarmID	Alarm OID	Alarm Severity	Alarm Type
4286849032	1.3.6.1.4.1.2011.5.25.667.2.37	Critical	Equipment alarm

Parameters

Name	Meaning
oid	Indicates the MIB object ID of the alarm.
RemoteUnitEsn	Indicates the ESN of the remote unit.

Impact on the System

The RU cannot work properly.

Possible Causes

The IIC channel of an RU is faulty.

Procedure

1. Check whether services are affected.
 - If so, go to step 2.
 - If not, go to step 4.
2. Restart the RU, and then check whether the alarm persists.
 - If so, go to step 3.
 - If not, go to step 5.
3. Replace the RU, and then check whether the alarm persists.
 - If so, go to step 4.
 - If not, go to step 5.
4. Collect alarm, log, and configuration information, and contact technical support personnel.
5. End.

3.3.269 ALM-4286849028 The remote-unit port is congested

Description

RUMNG/2/RUPORTCONGESTALARM: OID [oid] The remote unit interface is congested and packet loss may occur. (RemoteUnitEsn=[OCTET], InterfaceName=[OCTET])

The interface of the remote module is congested, and packet loss may have started.

Attribute

AlarmID	Alarm OID	Alarm Severity	Alarm Type
4286849028	1.3.6.1.4.1.2011.5.25.667.2.39	Warning	Quality of service alarm

Parameters

Name	Meaning
oid	Indicates the MIB object ID of the alarm.
RemoteUnitEsn	Indicates the ESN of the remote unit.
InterfaceName	Indicates the name of the interconnection interface.

Impact on the System

If this alarm is generated, the network is congested. If the fault is not rectified in time, network congestion will cause more packet loss, which will affect the normal running of services.

Possible Causes

The interface is congested.

Procedure

Collect alarm and configuration information, and contact technical support personnel.

3.3.270 ALM-3276800768 The CA certificate is nearly expired.

Description

PKI/4/PKICACERTNEARLYEXPIRED: OID [*oid*] the CA certificate is nearly expired. (CACertIssuer=[*issuer*], CACertSubject=[*subject*], CACertStartTime=[*starttime*], CACertFinishTime=[*finishtime*])

The CA certificate is about to expire.

Attribute

AlarmID	Alarm OID	Alarm Severity	Alarm Type
3276800768	1.3.6.1.4.1.2011.5.25.667.2.39	Warning	Communication alarm

Parameters

Name	Meaning
oid	Indicates the MIB object ID of the alarm.
CACertIssuer	Indicates the issuer of the CA certificate.
CACertSubject	Indicates the subject of the CA certificate.
CACertStartTime	Indicates the start time of the CA certificate.
CACertFinishTime	Indicates the end time of the CA certificate.

Impact on the System

The service will be invalid after the certificate expires.

Possible Causes

The CA certificate is about to expire. The CA certificate expiration time is less than the certificate expired prewarning time configured by the **pki set-certificate expire-prewarning** command.

Procedure

1. Run the **display clock** command to check whether the device time is correct. If not, run the **clock datetime** command in the user view to change the device time.
2. Apply for a new certificate through SCEP or CMPv2 online or apply for a new certificate offline.

3.3.271 ALM-3276800769 The local certificate is nearly expired

Description

PKI/4/PKILOCALCERTVALID: OID [*oid*] the local certificate is valid.
(LocalCertIssuer=[*issuer*], LocalCertSubject=[*subject*],
LocalCertStartTime=[*starttime*], LocalCertFinishTime=[*finishtime*])

The local certificate is valid.

Attribute

AlarmID	Alarm OID	Alarm Severity	Alarm Type
3276800769	1.3.6.1.4.1.2011.5. 25.667.2.39	Warning	Communication alarm

Parameters

Name	Meaning
oid	Indicates the MIB object ID of the alarm.
LocalCertIssuer	Indicates the issuer of the local certificate.
LocalCertSubject	Indicates the subject of the local certificate.
LocalCertStartTime	Indicates the start time of the local certificate.
LocalCertFinishTime	Indicates the end time of the local certificate.

Impact on the System

The service will be invalid after the certificate expires.

Possible Causes

The local certificate is about to expire. The local certificate expiration time is less than the certificate expired prewarning time configured by the **pki set-certificate expire-prewarning** command.

Procedure

1. Check whether the system time on the local device is correct.

2. If the system time is correct, apply for a new local certificate immediately.

3.3.272 ALM-3276800770 The peer device cannot go online because Eth-Trunk auto-negotiation fails

Description

ENTITYTRAP/4/PNP_TRUNK_FAILED: OID [oid] The peer device cannot go online because Eth-Trunk auto-negotiation fails. Check the configuration and connection. (PeerDeviceEsn=[STRING])

When Eth-Trunk auto-negotiation is performed in PnP mode, the negotiation failed on the peer device.

Attribute

AlarmID	Alarm OID	Alarm Severity	Alarm Type
3276800770	1.3.6.1.4.1.2011.5. 25.667.2.39	Major	Communication alarm

Parameters

Name	Meaning
oid	Indicates the MIB object ID of the alarm.
hwPeerDeviceEsn	Indicates the ESN of the peer device.

Impact on the System

Eth-Trunk link negotiation fails and the peer device cannot register with iMaster NCE-Campus and go online.

Possible Causes

The device connection is incorrect or the PnP configuration of the device is incorrect.

Procedure

1. Check whether the PnP configuration of the device is correct.
 - If the **pnnp startup-link-aggregation enable** command exists in the configuration file of the upstream device (that is, the local device), check whether the **pnnp startup-vlan send enable** command exists in the configuration file of the upstream device. If not, run the **pnnp startup-vlan send enable** command to enable the device to transmit PnP VLAN information to its downstream devices.

- Check whether the **undo pnp startup-vlan receive enable** command exists in the configuration file of the downstream device (that is, the peer device). If so, run the **pnp startup-vlan receive enable** command to enable the device to receive PnP VLAN negotiation packets from its upstream devices.
 - Check whether the **undo pnp startup-link-aggregation receive enable** command exists in the configuration file of the downstream device (that is, the peer device). If so, run the **pnp startup-link-aggregation receive enable** command to enable Eth-Trunk auto-negotiation.
2. Check whether the Eth-Trunk negotiation failure is caused by non-default configurations on the physical interface of the downstream device (that is, the peer device). If so, run the **undo** command to delete the non-default configurations.
 3. Check whether the ports on the upstream and downstream devices are correctly connected. If the connections are incorrect, Eth-Trunk negotiation will fail. In this case, correct the connections according to the plan.
 4. Collect alarm information and configuration information, and then contact technical support personnel.

3.3.273 ALM-4289601668 The board has been removed

Description

ENTITYTRAP/4/BOARDREMOVE: OID [oid] Board has been removed.
(Index=[INTEGER], EntityPhysicalIndex=[INTEGER], PhysicalName="[OCTET]", EntityTrapEntType=[INTEGER], EntityTrapFaultID=[INTEGER])

The board is removed.

Attribute

AlarmID	Alarm OID	Alarm Severity	Alarm Type
3276800770	1.3.6.1.4.1.2011.5.25.667.2.39	Warning	Equipment alarm

Parameters

Name	Meaning
oid	Indicates the MIB object ID of the alarm.
Index	Indicates the index.
EntityPhysicalIndex	Indicates the physical index.
PhysicalName	Indicates the entity name, such as SFU, LPU, and MPU. The entity name varies with the type of the board.

Name	Meaning
EntityTrapEntType	Indicates the entity type.
EntityTrapFaultID	Indicates the error code: 131840.

Impact on the System

If an LPU is removed, all services running on the LPU will be interrupted. If an MPU is removed, the system reliability will be affected. If a master MPU is removed, the master/slave switchover will occur, which interrupts all services in the system.

Possible Causes

The board has been removed.

Procedure

1. Check whether the board is removed for certain reasons, for example, routine maintenance.
 - If so, no action is required.
 - If not, go to step 2.
2. Check whether the slot ID in the alarm belongs to an MPU.
 - If so, go to step 4.
 - If not, go to step 3.
3. Determine whether to insert the board.
 - If so, go to step 4.
 - If not, no action is required.
4. Insert the corresponding board. After the board is started, run the **display device** command to check whether the board in the corresponding slot is registered successfully.
 - If so, no action is required.
 - If not, collect alarm information and configuration information, and then contact technical support personnel.

3.3.274 ALM-4289601669 The board has been inserted

Description

ENTITYTRAP/4/BOARDINSERT: OID [oid] Board has been inserted.
(Index=[INTEGER], EntityPhysicalIndex=[INTEGER], PhysicalName="[OCTET]", EntityTrapEntType=[INTEGER], EntityTrapFaultID=[INTEGER])

The board is inserted.

Attribute

AlarmID	Alarm OID	Alarm Severity	Alarm Type
4289601669	1.3.6.1.4.1.2011.5.25.667.2.39	Major	Equipment alarm

Parameters

Name	Meaning
oid	Indicates the MIB object ID of the alarm.
Index	Indicates the index.
EntityPhysicalIndex	Indicates the physical index.
PhysicalName	Indicates the entity name, such as SFU, LPU, and MPU. The entity name varies with the type of the board.
EntityTrapEntType	Indicates the entity type.
EntityTrapFaultID	Indicates the error code: 131840.

Impact on the System

None.

Possible Causes

The board has been inserted.

Procedure

This alarm message is informational only, and no action is required.

3.4 WAC&AP Alarms

3.4.1 ALM-303046722 The Communication with the RADIUS Authentication Server Was Resumed

Description

RDS/4/RDAUTHUP_WARNING:OID [OID] Communication with the RADIUS authentication server is resumed. (IP=[ip-address], Vpn-Instance:[vpn-instance-name])

The communication with the RADIUS authentication server was resumed.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046722	Warning	equipmentAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
ip-address	Indicates the IP address of the authentication server.
vpn-instance-name	Indicates the VPN Instance to which the authentication server belongs. This parameter is invalid.

Impact on the System

None

Possible Causes

- The communication with the RADIUS authentication server was resumed.
- The RADIUS authentication server restarted.

Procedure

This alarm is informational only, and no action is required.

3.4.2 ALM-303046723 The Communication with the RADIUS Authentication Server Was Interrupted

Description

RDS/4/RDAUTHDOWN_WARNING:OID [OID] Communication with the RADIUS authentication server is interrupted. (IP=[ip-address], Vpn-Instance:[vpn-instance-name])

The communication with the RADIUS authentication server was interrupted.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046723	Warning	equipmentAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
ip-address	Indicates the IP address of the authentication server.
vpn-instance-name	Indicates the VPN Instance to which the authentication server belongs. This parameter is invalid.

Impact on the System

The device cannot communicate with the RADIUS authentication server, which affects related services.

Possible Causes

The RADIUS authentication server was Down.

Procedure

- Step 1** Check whether the server is closed on the RADIUS authentication server.
- If so, no further action is required.
 - If not, go to step 2.
- Step 2** Check whether the RADIUS authentication server and the device can ping through each other to determine whether the link status is normal.
- If not, restore the link.
 - If so, go to step 3.
- Step 3** Run the **display radius-server configuration** command to check whether the configured shared key is correct.
- If the shared key is incorrect, you need to run the **radius-server shared-key cipher key-string** command to configure the shared key for the RADIUS server.
 - If the shared key is correct, go to step 4.
- Step 4** Contact technical support engineers.
- End

3.4.3 ALM-303046724 The Communication with the RADIUS Accounting Server Was Resumed

Description

RDS/4/RDACCTUP_WARNING:OID [OID] Communication with the RADIUS accounting server is resumed. (IP=[ip-address], Vpn-Instance:[vpn-instance-name])
The communication with the RADIUS accounting server was resumed.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046724	Warning	equipmentAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
ip-address	Indicates the IP address of the accounting server.
vpn-instance-name	Indicates the VPN Instance to which the accounting server belongs. This parameter is invalid.

Impact on the System

None

Possible Causes

- The communication with the RADIUS accounting server was resumed.
- The RADIUS accounting server restarted.

Procedure

This alarm is informational only, and no action is required.

3.4.4 ALM-303046725 The Communication with the RADIUS Accounting Server Was Interrupted

Description

RDS/4/RDACCTDOWN_WARNING:OID [OID] Communication with the RADIUS accounting server is interrupted. (IP=[ip-address], Vpn-Instance:[vpn-instance-name])

The communication with the RADIUS accounting server was interrupted.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046725	Warning	equipmentAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
ip-address	Indicates the IP address of the accounting server.
vpn-instance-name	Indicates the VPN Instance to which the accounting server belongs. This parameter is invalid.

Impact on the System

The device cannot communicate with the RADIUS accounting server, which affects related services.

Possible Causes

The RADIUS accounting server was Down.

Procedure

- Step 1** Check whether the RADIUS accounting server is closed.
- If so, no further action is required.
 - If not, go to step 2.
- Step 2** Check whether the RADIUS server and the device can ping through each other to determine whether the link is normal.

- If not, restore the link.
- If so, go to step 3.

Step 3 Run the **display radius-server configuration** command to check whether the configured shared key is correct.

- If not, run the **radius-server shared-key cipher** *key-string* command to configure the shared key for the RADIUS server.
- If so, go to step 4.

Step 4 Contact technical support engineers.

----End

3.4.5 ALM-303046721 The Percentage of Successfully Authenticated NAC Users Reached the Lower Alarm Threshold

Description

AAA/4/NACUserClearAlarm: OID [OID] The NAC Max User Alarm is cleared.(Slot:[OCTET] User-num:[INTEGER] Threshold:[INTEGER]%)

The percentage of successfully authenticated NAC users reached the lower alarm threshold.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046721	Warning	equipmentAlarm

Parameters

Name	Meaning
[OID]	Indicates the MIB object ID of the alarm.
Slot:[OCTET]	Indicates the slot ID.
User-num:[INTEGER]	Indicates the number of successfully authenticated NAC users.
Threshold:[INTEGER]%	Indicates the percentage of successfully authenticated NAC users.

Impact on the System

This is the clear alarm for the alarm generated when the percentage of successfully authenticated NAC users reaches the upper alarm threshold.

Possible Causes

The percentage of successfully authenticated NAC users reached or fell below the lower alarm threshold.

Procedure

This alarm is informational only, and no action is required.

3.4.6 ALM-303046720 The Percentage of Successfully Authenticated NAC Users Reached the Upper Alarm Threshold

Description

AAA/4/NACMaxUserAlarm: OID [OID] The number of NAC users reached the maximum.(Slot:[OCTET] User-num:[INTEGER] Threshold:[INTEGER]%)

The percentage of successfully authenticated NAC users reached the upper alarm threshold.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046720	Warning	equipmentAlarm

Parameters

Name	Meaning
[OID]	Indicates the MIB object ID of the alarm.
Slot:[OCTET]	Indicates the slot ID.
User-num:[INTEGER]	Indicates the number of successfully authenticated NAC users.
Threshold:[INTEGER]%	Indicates the percentage of successfully authenticated NAC users.

Impact on the System

None

Possible Causes

The percentage of successfully authenticated NAC users reached the upper alarm threshold.

Procedure

- Step 1** Run the **display authentication user-alarm configuration** command in any view to check the upper alarm threshold for the percentage of successfully authenticated NAC users. Adjust the threshold according to the network requirements. If the fault persists, go to step 2.
- Step 2** Collect log information and contact technical support engineers.
- End

3.4.7 ALM-303046736 The Number of Used Addresses in the IP Address Pool Reached the Upper Alarm Threshold

Description

AM/4/IPPOOLUSEDOUT: OID [OID] The number of used addresses exceeds alarm threshold. (PoolName=[OCTET], UsedPercentage=[OCTET])

The number of used addresses in the IP address pool reached the upper alarm threshold.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046736	Warning	equipmentAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
PoolName	Indicates the IP address pool name.
UsedPercentage	Indicates the percentage of used IP addresses in the IP address pool.

Impact on the System

IP addresses may fail to be allocated.

Possible Causes

The percentage of used addresses in the IP address pool reached the upper alarm threshold.

Procedure

- Reduce the mask length to add more allocatable IP addresses to the address pool. To reduce the mask length, run the **ip address ip-address { mask | mask-length }** command in the interface view or run the **network ip-address [mask { mask | mask-length }]** command in the global address pool view.
- If an IP address segment is configured in the address pool, increase the range of the IP address segment to add more allocatable IP addresses. To increase the range of the IP address segment, run the **dhcp server ip-range start-ip-address end-ip-address** command in the interface view or run the **section section-id start-address [end-address]** command in the global address pool view.

Related Information

None

3.4.8 ALM-303046737 The Number of Used Addresses in the IP Address Pool Reached the Lower Alarm Threshold

Description

AM/4/IPPOOLUSEDOUTRESUME: OID [OID] The number of used addresses descends to alarm threshold. (PoolName=[OCTET], UsedPercentage=[OCTET])

The number of used addresses in the IP address pool reached the lower alarm threshold.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046737	Warning	equipmentAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
PoolName	Indicates the IP address pool name.
UsedPercentage	Indicates the percentage of used IP addresses in the IP address pool.

Impact on the System

None

Possible Causes

The percentage of used addresses in the IP address pool reached the lower alarm threshold.

Procedure

This alarm is informational only, and no action is required.

Related Information

None

3.4.9 ALM-303046918 The ARP Packet Transmitting Rate Exceeded the Timestamp Suppression Rate Limit for ARP Packets

Description

ARP/4/ARP_SUPP_TRAP:OID [OID] Exceed the speed limit value configured. (Ifnet index=[INTEGER], Configured value=[COUNTER], Sampling value=[COUNTER], Speed-limit type=[OCTET],Source Ip address=[IPADDR], Destination Ip address=[IPADDR]).

The alarm was generated when the transmitting rate of ARP packets or ARP Miss messages was greater than the rate limit.

The alarm was cleared when the transmitting rate of ARP packets or ARP Miss messages was lower than the rate limit.

You can run the **arp speed-limit** command to set the rate limit. The default rate limit is 5 packets per second.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046918	Warning	processingErrorAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
Ifnet index	Indicates the interface index.
Configured value	Indicates the configured rate limit.

Name	Meaning
Sampling value	Indicates the sampling of the number of packets received within a period.
Speed-limit type	Indicates the type of packets configured with timestamp suppression, for example, ARP and ARP MISS.
Source Ip address	Indicates the source IP address.
Destination Ip address	Indicates the destination IP address.

Impact on the System

If ARP packets are configured with timestamp suppression, some normal ARP packets are discarded. As a result, traffic cannot be forwarded normally.

If ARP Miss messages are configured with timestamp suppression, some ARP Miss messages are discarded. As a result, ARP Request messages cannot be triggered and thus traffic cannot be forwarded normally.

If this alarm is cleared soon, services will not be affected and the system will return to normal state.

If this alarm is not cleared for a long time, service processing capabilities of the system will be affected.

Possible Causes

- The interval for enabling the log function and sending alarms for potential attack behaviors was set to Ns . Within the period of $N+1s$, the number of sent ARP packets was greater than the threshold. Within the first Ns , the average number of sent ARP packets was greater than the threshold.
- The interval for enabling the log function and sending alarms for potential attack behaviors was set to Ns . Within the period of $N+1s$, the number of sent ARP Miss messages was greater than the threshold. Within the first Ns , the average number of sent ARP Miss messages was greater than the threshold.

Procedure

- Step 1** View the type of packets configured with timestamp suppression in trap messages.
- If the type of packets is ARP, go to step 2.
 - If the type of packets is ARP Miss, go to step 4.
- Step 2** Run the **display arp anti-attack configuration** command to view the rate limit of ARP packets.
- Step 3** Run the **arp speed-limit source-ip [ip-address] maximum maximum** command to re-set the rate limit of timestamp suppression of ARP packets. This value must be greater than that displayed in step 2; otherwise, the trap cannot be cleared, but this value must be less than 32768. Then, check whether the trap is cleared.

- If so, no further action is required.
- If not, go to step 6.

Step 4 Run the **display arp anti-attack configuration** command to view the rate limit of ARP Miss messages.

Step 5 Run the **arp-miss speed-limit** [*ip-address*]**source-ip maximum** *maximum* command to re-set the maximum rate of timestamp suppression of ARP Miss messages. This value must be greater than that displayed in step 4; otherwise, the trap cannot be cleared, but this value must be less than 32768. Then, check whether the trap is cleared.

- If so, no further action is required.
- If not, go to step 6.

Step 6 Contact technical support engineers.

----End

Related Information

None

3.4.10 ALM-303046919 The Number of ARP Entries Exceeded the Upper Threshold

Description

ARP/4/ARP_THRESHOLD_EXCEED_TRAP:OID [OID] The number of ARP entries exceeded the threshold. (entPhysicalIndex=[INTEGER], Slot name=[OCTET], Threshold=[COUNTER], Number of dynamic ARP entries=[COUNTER], Number of static ARP entries=[COUNTER]).

The number of ARP entries exceeded the upper threshold.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046919	Warning	Quality of service alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
entPhysicalIndex	Indicates the index of a physical entity.
Slot name	Indicates the card name.
Threshold	Indicates the alarm threshold.

Name	Meaning
Number of dynamic ARP entries	Indicates the number of dynamic ARP entries.
Number of static ARP entries	Indicates the number of static ARP entries.

Impact on the System

If this alarm is displayed, the number of ARP entries on the device is great. If the number continuously increases, system resources become insufficient and no new ARP entries can be learned. As a result, service interruption may occur.

Possible Causes

The number of ARP entries on the device exceeded the upper threshold.

Procedure

- Step 1** Run the **display arp statistics** command to view ARP entry statistics on the device and check whether there are more static ARP entries or dynamic ARP entries.
- If there are more dynamic ARP entries, go to step 2.
 - If there are more static ARP entries, go to step 3.
- Step 2** Run the **display arp all** command to identify the interface that has more ARP entries. Then run the **display arp interface** command to check ARP entries on the interface and determine whether these ARP entries are necessary for the interface.
- If these ARP entries are necessary, go to step 5.
 - If these ARP entries are not necessary, run the **reset arp** command to delete specified ARP entries (without system running being affected) and go to step 4.
- Step 3** Run the **display current-configuration** command to view static ARP entries and check whether these static ARP entries are necessary.
- If these static ARP entries are necessary, go to step 5.
 - If these static ARP entries are not necessary, run the **undo arp static** command to delete specified static ARP entries (without system running being affected) or run the **reset arp static** command to clear all static ARP entries (without system running being affected). Then go to step 4.
- Step 4** Run the **display arp statistics** command to check whether the number of ARP entries still continuously increases unexpectedly.
- If the number of ARP entries does not continuously increase, no further action is required.
 - If the number of ARP entries still continuously increases, go to step 5.
- Step 5** Collect alarm information and configuration information, and then contact technical support engineers.

----End

Related Information

None

3.4.11 ALM-303046920 ARP Detects an IP Address Conflict

Description

ARP/4/ARP_IPCONFLICT_TRAP:OID [OID] ARP detects IP conflict. (IP address=[IPADDR], Local interface=[OCTET], Local MAC=[OCTET], Local vlan=[INTEGER], Local CE vlan=[INTEGER], Receive interface=[OCTET], Receive MAC=[OCTET], Receive vlan=[INTEGER], Receive CE vlan=[INTEGER], IP conflict type=[OCTET]).

An IP address conflict was detected by ARP.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046920	Warning	environmentalAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
IP address	Indicates the IP address that conflicts.
Local interface	Indicates the interface recorded in the ARP entry of the IP address.
Local MAC	Indicates the MAC address recorded in the ARP entry of the IP address.
Local vlan	Indicates the VLAN recorded in the ARP entry of the IP address.
Local CE vlan	Indicates the CE VLAN recorded in the ARP entry of the IP address.
Receive interface	Indicates the inbound interface of the second ARP packet with the IP address.
Receive MAC	Indicates the source MAC address of the second ARP packet with the IP address.
Receive vlan	Indicates the VLAN configured on the inbound interface of the second ARP packet with the IP address.

Name	Meaning
Receive CE vlan	Indicates the CE VLAN configured on the inbound interface of the second ARP packet with the IP address.
IP conflict type	Indicates the IP address conflict type.

Impact on the System

This alarm indicates that an IP address conflict occurred. If the IP address conflict is not eliminated timely, route flapping may occur and services may be interrupted.

Possible Causes

- The source IP address in an ARP packet is the same as the IP address of the inbound interface that receives the ARP packet, but the source MAC address in the ARP packet is different from the MAC address of the inbound interface.
- The source IP address in an ARP packet is the same as the IP address in an existing ARP entry, but the source MAC address is different from the MAC address in the ARP entry.
- The source IP address in an ARP packet is 0.0.0.0 (probe ARP packet), the destination IP address is the same as the IP address of the inbound interface that receives the ARP packet, but the source MAC address in the ARP packet is different from the MAC address of the inbound interface.

Procedure

Step 1 Identify the devices or users who use the same IP address.

- If the devices or users using the same IP address can be identified, change the IP address of one device or user. Then, go to step 2.
- If the devices or users using the same IP address cannot be identified, collect alarm information and configuration information, and then contact technical support engineers.

Step 2 Run the **display arp ip-conflict track** command to check whether there is any IP address conflict information, or check whether there is any alarm generated for IP address conflict.

- If there is any IP address conflict, go to step 1.
- If there is no IP address conflict, no further action is required.

----End

3.4.12 ALM-303046732 The Number of Global DHCP Users Reached the Upper Alarm Threshold

Description

DHCP/4/DHCPUSERBINDTRAPGLOBAL:OID [OID] The number of DHCP global users exceeds alarm threshold. (IfIndex=[INTEGER], VlanIndex=[INTEGER], CurrentUser=[INTEGER], MaxUser=[INTEGER])

The number of global DHCP users reached the upper alarm threshold.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046732	Warning	equipmentAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
IfIndex	Indicates the interface index. The value is 0 .
VlanIndex	Indicates the VLAN index. The value is 0 .
CurrentUser	Indicates the number of current access users.
MaxUser	Indicates the maximum number of access users.

Impact on the System

None

Possible Causes

The number of global DHCP snooping binding entries reached the upper alarm threshold.

Procedure

- Step 1** Run the **dhcp snooping max-user-number** *max-user-number* command to adjust the maximum number of access users allowed on the interface.

- Step 2** Run the **dhcp snooping user-alarm percentage** *percent-lower-value percent-upper-value* command to adjust the alarm thresholds.
- End

Related Information

None

3.4.13 ALM-303046733 The Number of Global DHCP Users Reached the Lower Alarm Threshold

Description

DHCP/4/DHCPUSERBINDTRAPGLOBALRESUME:OID [OID] The number of DHCP global users descends to alarm threshold. (IfIndex=[INTEGER], VlanIndex=[INTEGER], CurrentUser=[INTEGER], MaxUser=[INTEGER])

The number of global DHCP users reached the lower alarm threshold.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046733	Warning	equipmentAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
IfIndex	Indicates the interface index. The value is 0 .
VlanIndex	Indicates the VLAN index. The value is 0 .
CurrentUser	Indicates the number of current access users.
MaxUser	Indicates the maximum number of access users.

Impact on the System

None

Possible Causes

The number of global DHCP snooping binding entries reached the lower alarm threshold.

Procedure

- Step 1** Run the **dhcp snooping max-user-number** *max-user-number* command to adjust the maximum number of access users allowed on the interface.
- Step 2** Run the **dhcp snooping user-alarm percentage** *percent-lower-value percent-upper-value* command to adjust the alarm thresholds.

----End

Related Information

None

3.4.14 ALM-303046734 The Number of Global ND Users Reached the Upper Alarm Threshold

Description

DHCP/4/NDUSERBINDTRAPGLOBAL:OID [OID] The number of ND global users exceeds alarm threshold. (IfIndex=[INTEGER], VlanIndex=[INTEGER], CurrentUser=[INTEGER], MaxUser=[INTEGER])

The number of global ND users reached the upper alarm threshold.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046734	Warning	equipmentAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
IfIndex	Indicates the interface index. The value is 0.
VlanIndex	Indicates the VLAN index. The value is 0.
CurrentUser	Indicates the number of current access users.

Name	Meaning
MaxUser	Indicates the maximum number of access users.

Impact on the System

None

Possible Causes

The number of global ND snooping binding entries reached the upper alarm threshold.

Procedure

- Step 1

Run the **nd snooping max-user-number** *max-user-number* command to adjust the maximum number of ND snooping binding entries that can be learned by an interface.
- Step 2

Run the **nd snooping user-alarm percentage** *percent-lower-value percent-upper-value* command to configure the alarm thresholds for ND snooping binding entries.
- End

Related Information

None

3.4.15 ALM-303046981 The Number of Global ND Users Reached the Lower Alarm Threshold

Description

DHCP/4/NDUSERBINDTRAPGLOBALRESUME:OID [OID] The number of ND global users descends to alarm threshold. (IfIndex=[INTEGER], VlanIndex=[INTEGER], CurrentUser=[INTEGER], MaxUser=[INTEGER])

The number of global ND users reached the lower alarm threshold.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046981	Warning	equipmentAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
IfIndex	Indicates the interface index. The value is 0.
VlanIndex	Indicates the VLAN index. The value is 0.
CurrentUser	Indicates the number of current access users.
MaxUser	Indicates the maximum number of access users.

Impact on the System

None

Possible Causes

The number of global ND snooping binding entries reached the lower alarm threshold.

Procedure

- Step 1

Run the **nd snooping max-user-number** *max-user-number* command to adjust the maximum number of ND snooping binding entries that can be learned by an interface.
- Step 2

Run the **nd snooping user-alarm percentage** *percent-lower-value percent-upper-value* command to configure the alarm thresholds for ND snooping binding entries.
- End

Related Information

None

3.4.16 ALM-303046689 Device Temperature Reached the Threshold

Description

ENTITYTRAP/1/ENTITYBRDTEMPALARM:OID [OID] Temperature rise over or fall below the warning alarm threshold.
(Index=[INTEGER],EntryPhysicalIndex=[INTEGER], PhysicalName="[OCTET]",

EntityThresholdType=[INTEGER],EntityThresholdValue=[INTEGER],EntityThresholdCurrent=[INTEGER], EntityTrapFaultID=[INTEGER])

The device temperature exceeds the upper threshold or falls below the lower threshold. (You can run the **display temperature** command to view the alarm thresholds.)

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046689	Major	environmentalAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
Index	Indicates the index of a temperature sensor.
EntryPhysicalIndex	Indicates the sub-index of an entity.
PhysicalName	Indicates the entity name.
EntityThresholdType 1: rise over 2: fall below	Indicates the alarm type.
EntityThresholdValue	Indicates the alarm threshold.
EntityThresholdCurrent	Indicates the current temperature.
EntityTrapFaultID	Indicates the error code.

Impact on the System

Services on the cards may be affected if the temperature becomes too high.

Possible Causes

- The device was not ventilated well (for example, the air filter is blocked), which causes heat unable to be dissipated.
- The ambient temperature was high.
- One or more fans in the device failed.

 NOTE

ACU2 does not have a fan. Check the chassis fans or ambient temperature.

Procedure

- Step 1** Check whether the air filter of fans is blocked.
1. If so, clean the air filter or remove the blockage. After the device runs for a period, go to step 4.
 2. If not, go to step 2.
- Step 2** Check whether the ambient temperature is too high.
1. If so, lower the ambient temperature and go to step 4.
 2. If not, go to step 3.
- Step 3** Run the **display fan** command to check the fan state and rotation speed to determine whether the fan is faulty.
1. If so, rectify the fan fault or replace the fan. Then, go to step 4.
 2. If not, go to step 5.
- Step 4** Run the **display temperature all** command to check the device temperature.
1. If the temperature is normal, no further action is required.
 2. If the temperature is abnormal, go to step 5.
- Step 5** Collect trap, log, and configuration information, and contact technical support engineers.
- Step 6** If the alarm is cleared, no further action is required.
- End

Related Information

None

3.4.17 ALM-303046913 A Storage Card Was Removed

Description

ENTITYTRAP/4/STORAGEREMOVE:OID [OID] Storage remove.
(Index=[INTEGER],PhysicalName="[OCTET]",StorageName="[OCTET]")

This alarm was generated when a storage card was removed.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046913	Warning	equipmentAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
Index	Indicates the ID of an entity.
PhysicalName	Indicates the name of the entity.
StorageName	Indicates the storage device name.

Impact on the System

If the "is pulled out" alarm is displayed when the storage device is installed, the configuration file and log file may be lost.

Possible Causes

The storage device is pulled out.

Procedure

Check whether the storage device is removed. If not, contact technical support personnel.

Related Information

None

3.4.18 ALM-303046917 Some Functions on the Card Were Invalid

Description

ENTITYTRAP/2/BOARDFAIL: OID [OID] Board become failure for some reason. (Index=[INTEGER], EntityPhysicalIndex=[INTEGER], PhysicalName="[OCTET]", EntityTrapEntType= [INTEGER], EntityTrapFaultID=[INTEGER], EntityTrapReasonDescr="[OCTET]")

Some functions on the card are invalid.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046917	Major	equipmentAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm
Index	Indicates the entity index.
EntityPhysicalIndex	Indicates the physical entity index.
PhysicalName	Indicates the name of the physical entity.
EntityTrapEntType	Indicates the type of the physical entity, such as mpu(1), and lpu(2).
EntityTrapFaultID	Indicates the error code.
EntityTrapReasonDescr	Indicates the description of the alarm cause.

Impact on the System

The card is unavailable or some services are interrupted.

Possible Causes

Error Code	Possible Cause
132643	The Bluetooth function failed.
132642	The Reset button is faulty.
132641	The dual-edge connector is faulty.
132640	The CPU is faulty.
132623	The NP chip is faulty.
132103	The voltage failed.
132620	The power supply is faulty.
132619	The corrosion protection circuit is faulty.
132618	An overall fault occurs on the NP chip.
132149	The bad block rate for the NAND flash exceeds the threshold.
2125827	The temperature sensor is abnormal.

Error Code	Possible Cause
132865	The RTC was abnormal. NOTE When the RTC is faulty, the system time may be incorrect after the device is restarted. However, services indifferent to system timing are not affected. If an NTP server is available on the network, the system time will be corrected after you enable the NTP client function on the device.
132146	The PSE power supply is faulty.
132121	The current on the USB flash drive exceeds the upper limit.

Procedure (AC device)

Step 1 Check whether the faulty card is registered successfully and services are running properly.

Run the **display device** command to check whether the faulty card is registered successfully, and run the **display interface** command to view the statistics on received and sent packets. According to the statistics, check whether services are running properly.

- If the faulty card is registered successfully and services are running properly, no further action is required.
- If the faulty card is unregistered or services are not running properly, go to step 2.

Step 2 If the faulty card is a main control board, run the **reboot** command to reboot the device. Then check whether the device is working properly.

- If the card can be registered successfully and services are running properly, no further action is required.
- If the card cannot be registered or services cannot run properly, the card hardware is faulty. Replace this card.
- If the fault persists, go to step 3.

Step 3 Contact technical support engineers.

----End

Procedure (Cloud AP device)

Step 1 Check whether the faulty card is registered successfully and services are running properly.

Run the **display interface** command to view the statistics on received and sent packets. According to the statistics, check whether services are running properly.

- If the faulty card is registered successfully and services are running properly, no further action is required.

- If the faulty card is unregistered or services are not running properly, go to step 2.

Step 2 If the faulty card is a main control board, run the **reboot** command to reboot the device. Then check whether the device is working properly.

- If the card can be registered successfully and services are running properly, no further action is required.
- If the card cannot be registered or services cannot run properly, the card hardware is faulty. Replace this card.
- If the fault persists, go to step 3.

Step 3 Contact technical support engineers.

----End

Related Information

None

3.4.19 ALM-303046916 A Card Experienced A Complete Failure

Description

ENTITYTRAP/4/BOARDINVALID: OID [OID] Board is invalid for some reason.
(Index=[INTEGER], EntityPhysicalIndex=[INTEGER], PhysicalName="[OCTET]",
EntityTrapEntType= [INTEGER], EntityTrapFaultID=132624,
EntityTrapReasonDescr="[OCTET]")

A card experienced a complete failure.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046916	Warning	equipmentAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm
Index	Indicates the entity index.
EntityPhysicalIndex	Indicates the physical entity index.
EntPhysicalName	Indicates the name of the physical entity.
EntityTrapEntType	Indicates the type of the physical entity, such as mpu(1), and lpu(2).

Name	Meaning
EntityTrapFaultID	Indicates the error code.
EntityTrapReasonDescr	Indicates the description of the alarm cause.

Impact on the System

Services will be interrupted.

Possible Causes

Error Code	Possible Cause
132629	The PHY chip is abnormal.
132624	The ECC detects a memory error.
132614	The logic of the CPLD on the card is abnormal.
132616	The CPLD clock is faulty.
132148	The optical module is abnormal.
132622	The clock driver IIC is faulty.

Procedure (AC device)

Step 1 Check whether the faulty card is registered successfully and services are running properly.

Run the **display device** command to check whether the faulty card is registered successfully, and run the **display interface** command to view the statistics on received and sent packets. According to the statistics, check whether services are running properly.

- If the faulty card is registered successfully and services are running properly, no further action is required.
- If the faulty card is unregistered or services are not running properly, go to step 2.

Step 2 If the faulty card is a main control board, run the **reboot** command to reboot the device. Then check whether the device is working properly.

- If the card can be registered successfully and services are running properly, no further action is required.
- If the card cannot be registered or services cannot run properly, the card hardware is faulty. Replace this card.
- If the fault persists, go to step 3.

Step 3 Contact technical support engineers.

----End

Procedure (Cloud AP device)

Step 1 Check whether the faulty card is registered successfully and services are running properly.

Run the **display interface** command to view the statistics on received and sent packets. According to the statistics, check whether services are running properly.

- If the faulty card is registered successfully and services are running properly, no further action is required.
- If the faulty card is unregistered or services are not running properly, go to step 2.

Step 2 If the faulty card is a main control board, run the **reboot** command to reboot the device. Then check whether the device is working properly.

- If the card can be registered successfully and services are running properly, no further action is required.
- If the card cannot be registered or services cannot run properly, the card hardware is faulty. Replace this card.
- If the fault persists, go to step 3.

Step 3 Contact technical support engineers.

----End

Related Information

None

3.4.20 ALM-303046688 An Exception Occurred on the Card

Description

ENTITYTRAP/2/BOARDFAIL: OID [OID] Card become failure for some reason.
(Index=[INTEGER], EntityPhysicalIndex=[INTEGER], EntityTrapEntType= [INTEGER],
PhysicalName="[OCTET]", EntityTrapFaultID=[INTEGER])

An exception occurred on the card.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046688	Critical	equipmentAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object of the alarm.
Index	Indicates the entity index.
EntityPhysicalIndex	Indicates the index of the physical entity.
EntityTrapEntType	Indicates the entity type.
PhysicalName	Indicates the physical entity name.
EntityTrapFaultID	Indicates the error code.

Impact on the System

The card is unavailable, or some services are interrupted.

Possible Causes

Error Code	Possible Cause
132643	The Bluetooth function failed.
132642	The Reset button is faulty.
132641	The dual-edge connector is faulty.
132640	The CPU is faulty.
132623	The NP chip is faulty.
132103	The voltage failed.
132620	The power supply is faulty.
132619	The corrosion protection circuit is faulty.
132618	An overall fault occurs on the NP chip.
132149	The bad block rate for the NAND flash exceeds the threshold.
2125827	The temperature sensor is abnormal.

Error Code	Possible Cause
132865	The RTC was abnormal. NOTE When the RTC is faulty, the system time may be incorrect after the device is restarted. However, services indifferent to system timing are not affected. If an NTP server is available on the network, the system time will be corrected after you enable the NTP client function on the device.
132146	The PSE power supply is faulty.
132121	The current on the USB flash drive exceeds the upper limit.

Procedure

- Step 1**
Check whether the card is reset or powered off, or services on the card are not running properly.
 - If so, go to step 2.
 - If not, go to step 3.
- Step 2**
Power off and then on the card. Check whether the card fails to be registered or the fault persists after the card is registered.
 - If so, go to step 3.
 - If not, go to step 4.
- Step 3**
Collect alarms, logs, and configurations, and then contact technical support engineers.
- Step 4**
End.
- End

3.4.21 ALM-303046682 An Optical Module Was Removed from the AP

Description

ENTITYTRAP/4/OPTICALREMOVE:OID [OID] Optical Module has been removed. (Index=[INTEGER], EntityPhysicalIndex=[INTEGER], PhysicalName="[OCTET]", EntityTrapFaultID=[INTEGER])

An optical module was removed.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046682	Minor	equipmentAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm
Index	Indicates the index.
EntityPhysicalIndex	Indicates the physical index.
PhysicalName	Indicates the entity name, such as the interface name.
EntityTrapFaultID	Indicates the error code.

Impact on the System

None

Possible Causes

The optical module was removed.

Procedure

This alarm is informational only, and no action is required.

Related Information

[3.4.22 ALM-303046683 An Optical Module Was Installed on the AP](#)

3.4.22 ALM-303046683 An Optical Module Was Installed on the AP

Description

ENTITYTRAP/4/OPTICALINSERT:OID [OID] Optical Module has been inserted.
(Index=[INTEGER], EntityPhysicalIndex=[INTEGER], PhysicalName="[OCTET]", EntityTrapFaultID=[INTEGER])

An optical module was installed.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046683	Minor	equipmentAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm
Index	Indicates the index.
EntityPhysicalIndex	Indicates the physical index.
PhysicalName	Indicates the entity name, such as the interface name.
EntityTrapFaultID	Indicates the error code.

Impact on the System

None

Possible Causes

An optical module was installed.

Procedure

This alarm is informational only, and no action is required.

Related Information

[3.4.21 ALM-303046682 An Optical Module Was Removed from the AP](#)

3.4.23 ALM-303046960 The Optical Module Was Invalid

3.4.23.1 ALM-303046960 The Optical Module Was Invalid 136193

Description

ENTITYTRAP/4/OPTICALINVALID:OID [OID] Optical Module is invalid.
(Index=[INTEGER], EntityPhysicalIndex=[INTEGER], PhysicalName="[OCTET]", EntityTrapFaultID=136193)

The transmit power of the optical module reached the upper threshold.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046960	Warning	equipmentAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
Index	Indicates the index.
EntityPhysicalIndex	Indicates the physical entity index.
PhysicalName	Indicates the physical name.
EntityTrapFaultID	Indicates the error code.

Impact on the System

Services on the optical module may be affected, which probably leads to error codes, error packets, or even service interruption.

NOTE

This alarm takes effect only on Huawei-certified optical modules. This alarm may be incorrectly reported for non-Huawei certified optical modules if their internal diagnosis mechanism is incomplete.

Possible Causes

- The inserted optical module is a non-Huawei-customized optical module. If the optical module is delivered by Huawei earlier, this alarm may be generated because the manufacturer information is not recorded.
- The transmit power of the optical module is higher than the threshold specified by the vendor.
- The transmit power of the optical module is lower than the threshold specified by the vendor.
- The receive power of the optical module is higher than the threshold specified by the vendor.
- The receive power of the optical module is lower than the threshold specified by the vendor.
- The rate of the optical module does not match the rate of the corresponding interface. As a result, the interface cannot go Up.

Procedure

- Step 1** Check whether the optical fiber is faulty. If so, replace the optical fiber.
- Step 2** Check whether the model of the peer optical module matches that of the local optical module. If not, replace the local optical module with one that matches the peer one and has passed Huawei certification. Check whether the fault persists.
- Step 3** If the fault persists, collect alarms, logs, and configurations, and then contact technical support personnel.
- End

Related Information

None

3.4.24 ALM-303046915 The Power Supply Was Removed

Description

ENTITYTRAP/4/POWERREMOVE: OID [OID] Power has been removed.
(Index=[INTEGER], EntityPhysicalIndex=[INTEGER], PhysicalName="[OCTET]", EntityTrapFaultID=[INTEGER])

The power supply was removed.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046915	Warning	equipmentAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
Index	Indicates the index.
EntityPhysicalIndex	Indicates the physical entity index.
PhysicalName	Indicates the physical entity name.
EntityTrapFaultID	Indicates the error code.

Impact on the System

Cards cannot be powered on because the power supply is insufficient.

Possible Causes

The power supply was removed.

Procedure

- Step 1** Check whether the power supply was removed manually.
- If so, no further action is required.
 - If not, reinstall the power supply and go to step 2.
- Step 2** Run the **display power** command to check whether the power supply is present.
- If so, replace the power supply.
 - If not, go to step 3.
- Step 3** Contact technical support engineers.
- End

Related Information

None

3.4.25 ALM-303046409 The Power Supply Experienced a Partial Failure

Description

ENTITYTRAP/3/TRAPID_ENTITY_POWER_FAIL:OID [OID] Power become failure.
(EntityPhysicalIndex=[INTEGER], PhysicalName="[OCTET]
\",EntityTrapFaultID=[INTEGER],
EntityOperStatus=[INTEGER],EntityTrapReasonDescr="[OCTET]\")

The power supply may fail.

NOTE

This alarm is supported only by the AC6805.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046409	Major	equipmentAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object of the alarm.

Name	Meaning
EntityPhysicalIndex	Indicates the index of the physical entity.
PhysicalName	Indicates the physical entity name.
EntityTrapFaultID	Indicates the error code.
EntityOperStatus	Indicates the faulty status.
EntityTrapReasonDescr	Indicates the description of the alarm cause.

Impact on the System

The device may fail to run properly.

Possible Causes

Error Code	Possible Cause
136961	Voltage information failed to be obtained from the I2C interface.
136962	Overvoltage occurred.
136963	Undervoltage occurred.

Procedure

- Step 1

Replace the power supply and check whether the alarm persists.
 - If so, go to step 2.
 - If not, no further action is required.
- Step 2

Collect alarms, logs, and configurations, and then contact technical support engineers.
- End

Related Information

None

3.4.26 ALM-303046914 The Power Supply Was Invalid

Description

Entitytrap/4/POWERINVALID(t):OID [OID] Power is invalid for some reason.
(Index=[INTEGER], EntityPhysicalIndex=[INTEGER], PhysicalName=\"[OCTET]\", EntityTrapFaultID=136966)

The power supply is invalid.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046914	Warning	equipmentAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
Index	Indicates the index.
EntityPhysicalIndex	Indicates the index of the physical entity.
PhysicalName	Indicates the entity name, such as LPU and MPU. The entity name varies depending on the type of the card.
EntityTrapEntType	Indicates the entity type.
EntityTrapFaultID	Indicates the error code.

Impact on the System

Cards may fail to be powered on due to insufficient power supply.

Possible Causes

The power supply was installed but not powered on.

Procedure

Power on the power supply.

Related Information

None

3.4.27 ALM-303046690 CPU Usage Reached the Threshold

Description

ENTITYTRAP/2/CPUUSAGERISING: OID [OID] CPU utilization exceeded the pre-alarm threshold.(Index=[INTEGER], HwEntityPhysicalIndex=[INTEGER], PhysicalName="[OCTET]", EntityThresholdType=[INTEGER],

EntityThresholdWarning=[INTEGER], EntityThresholdCurrent=[INTEGER],
EntityTrapFaultID=[INTEGER])

The CPU usage reached the alarm threshold.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046690	Critical	equipmentAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object of the alarm.
Index	Indicates the entity index.
HwEntityPhysicalIndex	Indicates the physical entity index.
PhysicalName	Indicates the physical entity name.
EntityThresholdType	Indicates the threshold type.
EntityThresholdWarning	Indicates the alarm threshold.
EntityThresholdCurrent	Indicates the current value.
EntityTrapFaultID	Indicates the error code.

Impact on the System

The CPU usage exceeds the alarm threshold.

If the threshold is not high (for example, 50% or 60%), services are not affected. If the threshold is high (for example, 80%), high CPU usage in a very short period does not affect services; however, long-term high CPU usage may delay service processing.

Possible Causes

- The alarm threshold of the CPU usage was low.
- The traffic volume was high. For example, STAs frequently roam or go online or offline.
- The device provided too many services.
- The device was attacked, causing high CPU usage.

Procedure

- Step 1** Run the **display cpu-usage configuration** command to check the alarm threshold for CPU usage to determine whether the alarm threshold is set properly.

- If so, go to step 3.
- If not, go to step 2.

Step 2 Run the **set cpu-usage threshold** command to set a proper alarm threshold for CPU usage. After that, check whether the alarm persists.

- If so, go to step 3.
- If not, no further action is required.

Step 3 Check whether the traffic volume is high (for example, STAs frequently roam or a large number of STAs frequently go online or offline) and check whether the system runs properly if the traffic volume is high.

- If the traffic volume is high and the system runs normally, no further action is required.
- If the traffic volume is low, go to step 4.

Step 4 Run the **display cpu-usage** command in the diagnostic view to check the CPU usage of each task. Locate tasks with high CPU usage and delete unnecessary services or configurations to reduce the CPU usage.

- If the alarm persists after some services are deleted, go to step 4.
- If the alarm is cleared, no further action is required.

Step 5 Collect trap, log, and configuration information, as well as the CPU usage information in step 4, and contact technical support engineers.

----End

Related Information

None

3.4.28 ALM-303046691 Memory Usage Reached the Threshold

Description

ENTITYTRAP/2/MEMORYUSAGERISING: OID [OID] MEMORY utilization exceeded the pre-alarm threshold.(Index=[INTEGER], HwEntityPhysicalIndex=[INTEGER], PhysicalName="[OCTET]", EntityThresholdType=[INTEGER], EntityThresholdWarning=[INTEGER], EntityThresholdCurrent=[INTEGER], EntityTrapFaultID=[INTEGER])

The memory usage of the system reached the alarm threshold.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046691	Critical	equipmentAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object of the alarm.
Index	Indicates the entity index.
HwEntityPhysicalIndex	Indicates the physical entity index.
PhysicalName	Indicates the physical entity name.
EntityThresholdType	Indicates the threshold type.
EntityThresholdWarning	Indicates the alarm threshold.
EntityThresholdCurrent	Indicates the current value.
EntityTrapFaultID	Indicates the error code.

Impact on the System

If the threshold is not high (for example, 50% or 60%), services are not affected. If the threshold is high (for example, 80%), it may have the following impacts:

- Services cannot be allocated with memory and become unavailable.
- The storage medium has insufficient space, affecting log functions and software upgrades.

Possible Causes

- The memory alarm threshold was low.
- The device provided too many services.
- The device memory leaked.

Procedure

- Step 1** Run the **display memory-usage** command to check the alarm threshold for memory usage to determine whether the alarm threshold is set properly.
- If so, go to step 3.
 - If not, go to step 2.
- Step 2** Run the **set memory-usage threshold** command to set a proper alarm threshold for memory usage. After that, check whether the alarm persists.
- If so, go to step 3.
 - If not, no further action is required.
- Step 3** Delete unnecessary services and configurations to reduce memory usage.
- If this alarm persists, go to step 4.
 - If the alarm is cleared, no further action is required.

- Step 4** Collect alarms, logs, and configurations, and then contact technical support engineers.
- End

Related Information

None

3.4.29 ALM-303046964 Interface was deleted

Description

IFNET/4/IF_DELETE :OID [OID] Interface [interface-index] was deleted.
(InterfaceName=[STRING])

Interface was deleted.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046964	Warning	Communication alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
Interface-index	Indicates the interface index.
InterfaceName	Indicates the interface name.

Impact on the System

Services will not be affected.

Possible Causes

- Cause 1:
- This alarm is generated when a specified interface is deleted.

Procedure

- Step 1** This trap message is informational only, and no action is required.
- End

3.4.30 ALM-303046961 Interface input flow bandwidth usage exceeded the trap threshold

Description

IFNET/4/INBWRATEEXCEED: OID [OID] Interface input flow bandwidth usage exceeded the trap threshold. (Interface=[INTEGER], BandWidthUsage=[INTEGER], TrapThreshold=[INTEGER], InterfaceName=[STRING])

The trap was generated when the percentage of the rate of received traffic to the total bandwidth on an interface was greater than the threshold.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046961	Warning	environmentalAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
Interface	Indicates the interface index.
BandWidthUsage	Indicates bandwidth usage.
TrapThreshold	Indicates the trap threshold of bandwidth usage.
InterfaceName	Indicates the interface name.

Impact on the System

When the rate of traffic is close to 100% out of the total bandwidth, delay or packet loss will occur.

Possible Causes

The rate of traffic received by the interface was too large.

Procedure

- Step 1** Run the **display this interface** command on the interface to check whether the traffic threshold is too low. The threshold range is specified by users according to actual services.
- If so, go to Step 2.

- If not, go to Step 3.

Step 2 Run the **trap-threshold input-rate** *threshold_value* command to reset the threshold and then check whether the alarm is cleared.

- If so, go to Step 4.
- If not, go to Step 3.

Step 3 Collect alarm information and configuration information, and then contact technical support personnel.

Step 4 End.

----End

Related Information

[3.4.31 ALM-303046962 Interface output flow bandwidth usage exceeded the trap threshold](#)

3.4.31 ALM-303046962 Interface output flow bandwidth usage exceeded the trap threshold

Description

IFNET/4/INBWRATERESUME: OID [OID] Interface input flow bandwidth usage was restored to the trap threshold. (Interface=[INTEGER], BandWidthUsage=[INTEGER], TrapThreshold=[INTEGER], InterfaceName=[STRING])

The trap was generated when the percentage of the rate of received traffic to the total bandwidth on an interface became lower than the threshold.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046962	Warning	equipmentAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
Interface	Indicates the interface index.
BandWidthUsage	Indicates bandwidth usage.
TrapThreshold	Indicates the trap threshold of bandwidth usage.

Name	Meaning
InterfaceName	Indicates the interface name.

Impact on the System

None

Possible Causes

The rate of traffic received by the interface became lower than the threshold.

Procedure

Step 1 This alarm is informational only, and no action is required.

----End

Related Information

[3.4.30 ALM-303046961 Interface input flow bandwidth usage exceeded the trap threshold](#)

3.4.32 ALM-13049866 The link is disconnected

Description

IFNET/1/IF_LINKDOWN: OID [OID] Interface [interface-index] turned into DOWN state.(AdminStatus=[INTEGER],OperStatus=[INTEGER],InterfaceName=[OCTET])

The status of the link protocol on the interface became Down.

Attribute

Alarm ID	Alarm Severity	Alarm Type
13049866	Critical	equipmentAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
interface-index	Indicates the interface index.

Name	Meaning
AdminStatus	Indicates the admin status, which means whether the interface has been disabled. • 1: undo shutdown • 2: shutdown
OperStatus	Indicates the operating status, which means the link layer protocol status of the interface. • 1: Up • 2: Down
InterfaceName	Indicates the interface name.

Impact on the System

The interface cannot forward packets normally.

Possible Causes

Cause 1:

The interface became Down and the link was disconnected.

Cause 2:

The VLANIF interface is deleted.

Procedure

- Step 1** If the VLANIF interface is deleted, this trap message is informational only. No action is required, go to Step 7.
- Step 2** Run the **display this** command in the interface view to check whether interfaces on both ends are shut down.
 - If so, go to Step 3.
 - If not, go to Step 4.
- Step 3** Run the **undo shutdown** command in the interface view to check whether the alarm is cleared.
 - If so, go to Step 7.
 - If not, go to Step 4.
- Step 4** Check whether the cable and optical module are loosened or dropped.
 - If so, go to Step 6.
 - If not, go to Step 5.
- Step 5** Connect the physical link correctly and then check whether the alarm is cleared.

- If so, go to Step 7.
- If not, go to Step 6.

Step 6 Collect alarm information and configuration information, and then contact technical support personnel.

Step 7 End.

----End

Related Information

None

3.4.33 ALM-303046410 An IP address has been changed

Description

IP/4/IP_TRAPID_IPADDRESSCHANGE:OID [OID] An IP address has been changed. (OldIpAddress=[IPADDR], NewIpAddress=[IPADDR], IfIndex=[INTEGER], OldIpMask=[IPADDR], NewIpMask=[IPADDR], InterfaceName=[STRING])

An alarm was generated when the primary IP address of an interface was manually changed.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046410	Warning	equipmentAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
OldIpAddress	Original IP address
NewIpAddress	New IP address
IfIndex	Interface index
OldIpMask	Original IP address mask
NewIpMask	New IP address mask
InterfaceName	Interface name

Impact on the System

If the IP address is changed, services may be interrupted.

Possible Causes

The primary IP address of an interface was manually changed.

Procedure

The alarm is informational only, and no action is required.

Related Information

None

3.4.34 ALM-303046742 An IPSec tunnel is established

Description

IPSEC/4/IPSECTUNNELSTART: OID [OID] The IPSec tunnel is established.
(Ifindex=[Ifindex], SeqNum=[SeqNum],TunnelIndex=[TunnelIndex],
RuleNum=[RuleNum], DstIP=[DstIP], InsideIP=[InsideIP],
RemotePort=[RemotePort], CpuID=[CpuID], SrcIP=[SrcIP], FlowInfo=[FlowInfo],
LifeSize=[LifeSize], LifeTime=[LifeTime], VsysName=[vsys-name],
InterfaceName=[InterfaceName], SlotID=[SlotID], Role=[Role])

An IPSec tunnel is established.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046742	Warning	Communication alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
Ifindex	Indicates the interface index.
SeqNum	Indicates the policy number.
TunnelIndex	Indicates the tunnel index.
RuleNum	Indicates the rule number.
DstIP	Indicates the IP address of the peer end of the IPSec tunnel.
InsideIP	Indicates the intranet IP address of the peer end of the tunnel.

Name	Meaning
RemotePort	Indicates the port number of the peer end of the IPsec tunnel.
CpuID	Indicates the CPU number.
SrcIP	Indicates the IP address of the local end of the IPsec tunnel.
FlowInfo	Indicates the data flow information of the IPsec tunnel, including the source address, destination address, ACL port number, ACL protocol number, and DSCP.
LifeSize	Indicates the life cycle of the tunnel, in kbytes.
LifeTime	Indicates the life cycle of the tunnel, in seconds.
vsys-name	Indicates the name of the virtual system to which the IPsec policy belongs. NOTE The device does not support this parameter.
InterfaceName	Indicates the interface name.
SlotID	Indicates the Slot number. NOTE The device does not support this parameter.
Role	Device role during SA negotiation: • Initiator: The device functions as the SA negotiation initiator. • Responder: The device functions as the SA negotiation responder.

Impact on the System

None

Possible Causes

When an IPsec tunnel is established successfully, the alarm is generated.

Procedure

- This trap message is informational only, and no action is required.

Related Information

3.4.35 ALM-303046743 An IPSec tunnel is deleted

3.4.35 ALM-303046743 An IPSec tunnel is deleted

Description

IPSEC/4/IPSECTUNNELSTOP: OID [OID] The IPSec tunnel is deleted.
(Ifindex=[Ifindex], SeqNum=[SeqNum],TunnelIndex=[TunnelIndex],
RuleNum=[RuleNum], DstIP=[DstIP], InsideIP=[InsideIP],
RemotePort=[RemotePort], CpuID=[CpuID], SrcIP=[SrcIP], FlowInfo=[FlowInfo],
OfflineReason=[offlinereason], VsysName=[vsys-name],
InterfaceName=[InterfaceName], SlotID=[SlotID])

An IPSec tunnel is deleted.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046743	Warning	Communication alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
Ifindex	Indicates the interface index.
SeqNum	Indicates the policy number.
TunnelIndex	Indicates the tunnel index.
RuleNum	Indicates the rule number.
DstIP	Indicates the IP address of the peer end of the IPSec tunnel.
InsideIP	Indicates the intranet IP address of the peer end of the tunnel.
RemotePort	Indicates the port number of the peer end of the IPSec tunnel.
CpuID	Indicates the CPU number.
SrcIP	Indicates the IP address of the local end of the IPSec tunnel.

Name	Meaning
FlowInfo	Indicates the data flow information of the IPsec tunnel, including the source address, destination address, ACL port number, ACL protocol number, and DSCP.
offlinereason	Indicates the reason why the IPsec tunnel was deleted.
vsys-name	Indicates the name of the virtual system to which the IPsec policy belongs. NOTE The device does not support this parameter.
InterfaceName	Indicates the interface name.
SlotID	Indicates the Slot number. NOTE The device does not support this parameter.

Impact on the System

An IPsec tunnel has been deleted.

Possible Causes

An IPsec tunnel has been deleted due to the following causes:

- dpd timeout: Dead peer detection (DPD) times out.
- peer request: The remote end has sent a message, asking the local end to tear down the tunnel.
- config modify or manual offline: An SA is deleted due to configuration modification or an SA is manually deleted.
- phase1 hard expiry: Hard lifetime expires in phase 1 (no new SA negotiation success message is received).
- phase2 hard expiry: Hard lifetime expires in phase 2.
- heartbeat timeout: heartbeat detection times out.
- re-auth timeout: An SA is deleted due to reauthentication timeout.
- aaa cut user: The AAA module disconnects users.
- hard expiry triggered by port mismatch: A hard timeout occurs due to mismatch NAT port number.
- kick old sa with same flow: The old SA is deleted for the same incoming flow.
- spi conflict: An SPI conflict occurs.
- phase1 sa replace: The new IKE SA replaces the old IKE SA.

- phase2 sa replace: The new IPsec SA replaces the old IPsec SA.
- receive invalid spi notify: The device receives an invalid SPI notification.
- dns resolution status change: DNS resolution status changes.
- ikev1 phase1-phase2 sa dependent offline: The device deletes the associated IPsec SA when deleting an IKEv1 SA.
- exchange timeout: Packet interaction timeout.

Procedure

- Cause: dpd timeout
Perform the ping operation to check link reachability. If the link is unreachable, check the link and network configuration.
- Cause: heartbeat timeout
 - a. Perform the ping operation to check link reachability. If the link is unreachable, check the link configuration.
 - b. Check the heartbeat configuration on the two ends. If the configuration is incorrect, correct it.
- Cause: config modify or manual offline
 - a. Check whether the tunnel is deleted manually or whether the SA is reset. If so, no operation is required.
 - b. Check whether the IPsec configuration modified on the local end is correct. If not, correct the IPsec configuration.
 - c. Check whether manually deleted IPsec policies are redundant. If they are not redundant, reapply IPsec policies to the interface.
- Cause: phase1 hard expiry
Check whether the IKE SA lifetime is proper. If not, modify the IKE SA lifetime.
- Cause: phase2 hard expiry
Check whether the IPsec SA lifetime is proper. If not, modify the IPsec SA lifetime.
- Cause: hard expiry triggered by port mismatch
Check whether the two ends use the same NAT port number. If not, modify the NAT port numbers to be the same.
- Cause: peer request
Check log information of the remote device and determine the causes for the IPsec tunnel fault accordingly.
- Cause: receive invalid spi notify
If this fault occurs frequently, check whether the remote device status or configurations are abnormal.
- Cause: dns resolution status change
 - a. Ensure that the link between the device and DNS server is normal.
 - b. Ensure that the DNS server is working properly.
 - c. Ensure that the domain name configured using the **remote-address host-name** command is correct.
- Cause: ikev1 phase1-phase2 sa dependent offline

This symptom is normal and no operation is required if the devices at two ends can renegotiate the IKE SA and IPsec SA. Otherwise, you are advised to run the **undo ikev1 phase1-phase2 sa dependent** command on the local device to cancel dependency between IPsec SA and IKE SA during IKEv1 negotiation.

- Cause: exchange timeout
Ensure that the link is normal and the IPsec configuration is correct.
- Cause: kick old sa with same flow
Run the **ipsec remote traffic-identical accept** command to allow branch or other users to quickly access the headquarters network.
- Cause: aaa cut user, re-auth timeout, phase1 sa replace, phase2 sa replace, spi conflict
This symptom is normal and no operation is required.

Related Information

[3.4.34 ALM-303046742 An IPsec tunnel is established](#)

3.4.36 ALM-303046744 An IPsec policy is added

Description

IPSEC/4/IPSECPOLICYADD: OID [OID] An IPsec policy is added.
(SeqNum=[sequence-number], PolicyName=[policy-name], VsysName=[vsys-name])
An IPsec policy is added.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046744	Warning	Communication alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
sequence-number	Indicates the number of the IPsec policy.
policy-name	Indicates the name of the IPsec policy.

Name	Meaning
vsys-name	Indicates the name of the virtual system to which the IPsec policy belongs. NOTE The device does not support this parameter.

Impact on the System

None

Possible Causes

When an IPsec policy is added, the alarm is generated.

Procedure

- This log message is informational only, and no action is required.

Related Information

[3.4.37 ALM-303046745 An IPsec policy is deleted](#)

3.4.37 ALM-303046745 An IPsec policy is deleted

Description

IPSEC/4/IPSECPOLICYDEL: OID [OID] An IPsec policy is deleted.
(SeqNum=[sequence-number], PolicyName=[policy-name], VsysName=[vsys-name])

An IPsec policy is deleted.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046745	Warning	Communication alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.

Name	Meaning
sequence-number	Indicates the number of the IPSec policy.
policy-name	Indicates the name of the IPSec policy.
vsys-name	Indicates the name of the virtual system to which the IPSec policy belongs. NOTE The device does not support this parameter.

Impact on the System

None

Possible Causes

When an IPSec policy is deleted, the alarm is generated.

Procedure

- This log message is informational only, and no action is required.

Related Information

[3.4.36 ALM-303046744 An IPSec policy is added](#)

3.4.38 ALM-303046746 An IPSec policy is applied to an interface

Description

IPSEC/4/IPSECPOLICYATTACH: OID [OID] An IPSec policy is applied to an interface. (IfIndex=[interface-index], PolicyName=[policy-name], VsysName=[vsys-name], InterfaceName=[interface-name])

An IPSec policy is applied to an interface.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046746	Warning	Communication alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
interface-index	Indicates the index of the interface to which the IPsec policy is applied.
policy-name	Indicates the name of the applied IPsec policy.
vsys-name	Indicates the name of the virtual system to which the IPsec policy belongs. NOTE The device does not support this parameter.
interface-name	Indicates the interface name.

Impact on the System

None

Possible Causes

When an IPsec policy is applied to an interface, the alarm is generated.

Procedure

- This trap message is informational only, and no action is required.

Related Information

[3.4.39 ALM-303046747 The application of an IPsec policy is deleted from an interface](#)

3.4.39 ALM-303046747 The application of an IPsec policy is deleted from an interface

Description

IPSEC/4/IPSECPOLICYDETACH: OID [OID] An IPsec policy is cancelled on an interface. (IfIndex=[interface-index], PolicyName=[policy-name], VsysName=[vsys-name], InterfaceName=[interface-name])

The application of an IPsec policy is deleted from an interface.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046747	Warning	Communication alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
interface-index	Indicates the index of the interface to which the IPSec policy is deleted.
policy-name	Indicates the name of the deleted IPSec policy.
vsys-name	Indicates the name of the virtual system to which the IPSec policy belongs. NOTE The device does not support this parameter.
interface-name	Indicates the interface name.

Impact on the System

If tunnels exist, the running tunnel is disconnected.
If no tunnels exist, services are not affected.

Possible Causes

When the application of an IPSec policy is deleted from an interface, the alarm is generated.

Procedure

- This trap message is informational only, and no action is required.

Related Information

[3.4.38 ALM-303046746 An IPSec policy is applied to an interface](#)

3.4.40 ALM-303046748 Reset IKE SA

Description

IPSEC/4/IPSECRESETIKESA: OID [OID] Reset IKE SA. (VsysName=[vsys-name])

Reset IKE SA.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046748	Warning	Communication alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
vsys-name	Indicates the name of the virtual system to which the IKE SA belongs. NOTE The device does not support this parameter.

Impact on the System

The IPSec user is disconnected, and services are affected.

Possible Causes

This log message is generated when the **reset ike sa** command is executed.

Procedure

- This log message is informational only, and no action is required.

3.4.41 ALM-303046749 Reset IPSec SA

Description

IPSEC/4/IPSECRESETIPSECSA: OID [*OID*] Reset IPSec SA. (VsysName=[*vsys-name*])

Reset IPSec SA.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046749	Warning	Communication alarm

Parameters

Name	Meaning
<i>OID</i>	Indicates the MIB object ID of the alarm.
<i>vsys-name</i>	Indicates the name of the virtual system to which the IPsec SA belongs. NOTE The device does not support this parameter.

Impact on the System

The IPsec user is disconnected, and services are affected.

Possible Causes

This log message is generated when the **reset ipsec sa** command is executed.

Procedure

- This log message is informational only, and no action is required.

3.4.42 ALM-303046750 The number of IPsec tunnels has reached 80% of the CPU or license limit threshold

Description

IPSEC/4/IPSECREACHMAXTUNNEL: OID [OID] Current counts of ipsec tunnel will reach max CPU limit or license limit, please check it.

The number of IPsec tunnels has reached 80% of the CPU or license limit threshold.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046750	Warning	Communication alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.

Impact on the System

New tunnels cannot be set up after the number of IPsec tunnels reaches the threshold.

Possible Causes

The number of IPsec tunnels has reached 80% of the CPU or license limit threshold.

Procedure

Step 1 Expand the CPU capacity or apply for a new license.

----End

3.4.43 ALM-303046751 The number of IPsec tunnels has reached 90% of the CPU or license limit threshold

Description

IPSEC/4/IPSECREACHMAXTUNNELATONCE: OID [OID] Current counts of ipsec tunnel will reach max CPU limit or license limit, please check it at once.

The number of IPsec tunnels has reached 90% of the CPU or license limit threshold.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046751	Warning	Communication alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.

Impact on the System

New tunnels cannot be set up after the number of IPsec tunnels reaches the threshold.

Possible Causes

The number of IPsec tunnels has reached 90% of the CPU or license limit threshold.

Procedure

Step 1 Expand the CPU capacity or apply for a new license.

----End

3.4.44 ALM-303046752 The number of IKE peers dynamically created by the AC has reached 80% of the threshold

Description

IPSEC/4/IKEREACHMAXPEER: OID [OID] Current counts of ike peer will reach max limit.

The number of IKE peers dynamically created by the AC has reached 80% of the threshold.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046752	Warning	Communication alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.

Impact on the System

New IKE peers cannot be created after the number of dynamically created IKE peers reaches the threshold.

Possible Causes

The number of IKE peers dynamically created by the firewall has reached 80% of the threshold.

Procedure

Step 1 Check the IKE peers connected to the headquarters to see whether there are any unauthorized connections. If so, remove the unauthorized connections.

----End

3.4.45 ALM-303046753 The number of IKE peers dynamically created by the firewall has reached 90% of the threshold

Description

IPSEC/4/IKEREACHMAXPEERATONCE: OID [OID] Current counts of ike peer reach max limit.

The number of IKE peers dynamically created by the firewall has reached 90% of the threshold.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046753	Warning	Communication alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.

Impact on the System

New IKE peers cannot be created after the number of dynamically created IKE peers reaches the threshold.

Possible Causes

The number of IKE peers dynamically created by the firewall has reached 90% of the threshold.

Procedure

- Step 1** Check the IKE peers connected to the headquarters to see whether there are any unauthorized connections. If so, remove the unauthorized connections.

----End

3.4.46 ALM-303046754 The IKE SA has been established

Description

IPSEC/4/IKESAPHASE1ESTABLISHED: OID [OID] IKE phase1 sa established.
(PeerAddress=[PeerAddress], PeerPort=[PeerPort], LocalAddress=[LocalAddress], AuthMethod=[AuthMethod], AuthID=[AuthID], IDType=[IDType], VsysName=[vsys-name], Role=[Role])

The IKE SA has been established.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046754	Warning	Communication alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
PeerAddress	Indicates the IP address of the tunnel's remote end.
PeerPort	Indicates the port number of the peer end of the IPsec tunnel.
LocalAddress	Indicates the IP address of the tunnel's local end.
AuthMethod	Indicates the authentication method.
AuthID	Indicates the ID of the tunnel's remote end.
IDType	Indicates the type of the remote end ID.
vsys-name	Indicates the name of the virtual system to which the IKE SA belongs. NOTE The device does not support this parameter.
Role	Device role during SA negotiation: - Initiator: The device functions as the SA negotiation initiator. - Responder: The device functions as the SA negotiation responder.

Impact on the System

Services are not affected.

Possible Causes

The IKE SA has been established.

Procedure

- This log message is informational only, and no action is required.

3.4.47 ALM-303046756 The number of IPSec tunnels has reached the limit supported by a single CPU or license

Description

IPSEC/4/IPSECREACHMAXTUNNELMAX: OID [OID] Current counts of ipsec tunnel has been reached max CPU limit or license limit, please check it at once.

The number of IPSec tunnels has reached the limit supported by a single CPU or license.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046756	Warning	Communication alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.

Impact on the System

New tunnels cannot be set up after the number of IPSec tunnels reaches the limit.

Possible Causes

The number of IPSec tunnels has reached the limit.

Procedure

Step 1 Delete unnecessary IPSec tunnels.

Step 2 Expand CPU capacity or apply for a new license.

----End

3.4.48 ALM-303046755 IPSec tunnel negotiation fails

Description

IPSEC/4/IPSECNEGOFAIL: OID [OID] IPSec tunnel negotiation fails.
(Ifindex=[Ifindex], SeqNum=[SeqNum], Reason=[Reason],

ReasonCode=[ReasonCode], PeerAddress=[PeerAddress], PeerPort=[PeerPort],
VsysName=[vsys-name], InterfaceName=[InterfaceName], ConnID=[ConnID])

IPSec tunnel negotiation fails.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046755	Warning	Communication alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
Ifindex	Indicates the index of the interface on the IPSec tunnel.
SeqNum	Indicates the sequence number of the IPSec policy.
Reason	Indicates the reason of IPSec tunnel negotiation failure.

Name	Meaning
ReasonCode	Indicates the reason code of IPSec tunnel negotiation failure. • 1: phase1 proposal mismatch • 2: phase2 proposal or pfs mismatch • 3: encapsulation mode mismatch • 4: flow or peer mismatch • 5: version mismatch • 6: responder dh mismatch • 7: initiator dh mismatch • 12: peer address mismatch • 13: config ID mismatch • 14: construct local ID fail • 15: authentication fail • 16: rekey no find old sa • 17: rekey fail • 18: first packet limited • 21: invalid cookie • 24: invalid length • 26: unsupported version • 28: malformed payload • 30: malformed message • 31: cookie mismatch • 32: exchange mode mismatch • 33: unknown exchange type • 34: critical drop • 35: uncritical drop • 36: route limit • 39: local address mismatch • 40: nat detection fail • 41: ipsec tunnel number reaches limitation • 42: dynamic peers number reaches limitation • 46: flow conflict • 48: netmask mismatch • 49: no policy applied on interface • 50: fragment packet limit • 51: fragment packet reassemble timeout • 52: form cert payload fail

Name	Meaning
	• 53: max transmit reached • 54: no valid local cert
PeerAddress	Indicates the remote IP address.
PeerPort	Indicates the remote UDP port number.
vsys-name	Indicates the name of the virtual system to which the IPsec policy belongs. NOTE The device does not support this parameter.
InterfaceName	Indicates the interface name.
ConnID	Indicates the connection ID of an SA.

Impact on the System

Creating an IPsec tunnel will fail.

Possible Causes

The possible causes are as follows:

- phase1 proposal mismatch: IKE proposal parameters of the two ends do not match.
- phase2 proposal or pfs mismatch: IPsec proposal parameters or pfs algorithm of the two ends do not match.
- responder dh mismatch: The DH algorithm of the responder does not match.
- initiator dh mismatch: The DH algorithm of the initiator does not match.
- encapsulation mode mismatch: The encapsulation mode does not match.
- flow or peer mismatch: The security ACL or IKE peer address of the two ends does not match.
- version mismatch: The IKE version number of the two ends does not match.
- peer address mismatch: The IKE peer address of the two ends does not match.
- config ID mismatch: The IKE peer of the specified ID is not found.
- exchange mode mismatch: The negotiation mode of the two ends does not match.
- authentication fail: Identity authentication fails.
- construct local ID fail: The local ID fails to be constructed.
- rekey no find old sa: The old SA is not found during re-negotiation.
- rekey fail: The old SA is going offline during re-negotiation.
- first packet limited: The rate of the first packet is limited.

- unsupported version: The IKE version number is not supported.
- malformed message: Malformed message.
- malformed payload: Malformed payload.
- critical drop: Unidentified critical payload.
- cookie mismatch: Cookie mismatch.
- invalid cookie: Invalid cookie.
- invalid length: Invalid packet length.
- unknown exchange type: Unknown negotiation mode.
- route limit: The number of injected routes has reached the upper limit.
- local address mismatch: The local IP address in IKE negotiation and interface IP address do not match.
- dynamic peers number reaches limitation: The number of IKE peers reaches the upper limit.
- ipsec tunnel number reaches limitation: The number of IPSec tunnels reaches the upper limit.
- netmask mismatch: The mask does not match the configured mask after the IPSec mask filtering function is enabled.
- flow conflict: A data flow conflict occurs.
- no policy applied on interface: No policy is applied to an interface.
- nat detection fail: NAT detailed failed.
- fragment packet limit: Fragment packets exceed the limit.
- fragment packet reassemble timeout: Fragment packet reassembly times out.

Procedure

- Cause: phase1 proposal mismatch
Check IKE proposal parameters at both ends of the IPSec tunnel and ensure that the parameters are consistent at both ends.
- Cause: phase2 proposal or pfs mismatch
Check IPSec proposal parameters or PFS algorithms at both ends of the IPSec tunnel and ensure that the parameters or algorithms are consistent at both ends.
- Cause: responder dh mismatch, initiator dh mismatch
Check DH algorithms at both ends of the IPSec tunnel and ensure that the algorithms are consistent at both ends.
- Cause: encapsulation mode mismatch
Check encapsulation modes at both ends of the IPSec tunnel and ensure that the encapsulation modes are consistent at both ends.
- Cause: peer address mismatch
Check the IP addresses of IKE peers at both ends and ensure that the IP addresses match each other.
- Cause: config ID mismatch
Check identity authentication parameters, such as the ID type and ID value, and ensure that the parameters match each other.

- Cause: authentication fail
Check IKE proposal parameters or IKE peer parameters at both ends of the IPSec tunnel and ensure that the parameters are consistent at both ends.
- Cause: exchange mode mismatch
Check the IKEv1 phase 1 negotiation modes at both ends and ensure that the negotiation modes are consistent at both ends.
- Cause: route limit
Replace the device with the one that has a higher route specification and plan the network properly.
- Cause: local address mismatch
Check the local IP address and interface IP address used in IKE negotiation and ensure that the IP addresses are consistent.
- Cause: ipsec tunnel number reaches limitation
Delete unnecessary IPSec tunnels or expand the capacity.
- Cause: dynamic peers number reaches limitation
Expand the capacity and plan the network properly.
- Cause: flow conflict
Check ACL rules at both ends of the IPSec tunnel and ensure that the ACLs are correct.
- Cause: netmask mismatch
Change the IPSec-protected data flow range of the branch or headquarters to ensure that the data flow ranges negotiated by the branch and headquarters do not overlap.
- Cause: no policy applied on interface
Apply the required IPSec policy to the interface.
- Cause: fragment packet limit
The number of received fragmented packets exceeds the limit. Adjust the MTU of the peer device correctly.
- Cause: fragment packet reassemble timeout
Ensure that the links at both ends are normal and the device status is normal.
- Cause: max transmit reached
Check whether the network environment is normal.
- Cause: no valid local cert
Use a valid CA or local certificate.
- If the fault persists, collect related information and contact technical support personnel.

3.4.49 ALM-303046977 An Interface Receives a Packet with an Insecure MAC Address

Description

L2IFPPI/4/PORTACTIONTRAP:OID [*OID*] Interface ([*INTEGER1*]/[*INTEGER2*]) [*OCTET*] receive insecure mac-address, and the port status is : [*INTEGER*].
(1:restrict;2:protect;3:shutdown)

An interface receives a packet with an insecure MAC address.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046977	Warning	Quality of service alarm

Parameters

Name	Meaning
<i>OID</i>	Indicates the MIB object ID of the alarm.
[<i>INTEGER1</i>]/[<i>INTEGER2</i>]	Indicates the interface index.
<i>OCTET</i>	Indicates the interface name.
<i>INTEGER3</i>	Indicates the interface status.

Impact on the System

Traffic transmission on an interface is affected.

Possible Causes

Cause 1:

The number of MAC address entries reaches the threshold.

Procedure

Step 1 Check the port status.

- If the port is in restrict state, go to step 2.
- If the port is in shutdown state, go to step 3.

Step 2 Run the **port-security max-mac-num** *max-number* command to increase the maximum number of secure dynamic MAC addresses that can be learned by an interface. Then check whether the traffic transmission is normal.

- If yes, go to step 5.
- If not, go to step 4.

Step 3 Run the **undo shutdown** command. Then check whether the traffic transmission is normal.

- If yes, go to step 5.
- If not, go to step 4.

Step 4 Contact technical support personnel.

Step 5 End.

----End

Related Information

None

3.4.50 ALM-303046968 Receive illegal MAC

Description

L2IFPPI/4/ILLEGAL_MAC_TRAP: OID [OID] Receive illegal MAC [OCTET].

The interface receives a packet with an all-0 destination or source MAC address.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046968	Warning	Quality of service alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
OCTET	Indicates the alarm cause.

Impact on the System

None

Possible Causes

Cause 1: The interface receives an all-0 source MAC address.

Cause 2: The interface receives an all-0 destination MAC address.

Procedure

- After receiving the first packet with an all-0 source MAC address or destination MAC address, the device discards the packet and sends an alarm

to the NMS. When receiving other packets with the same MAC address, the device does not send any alarm to the NMS and discards the packets directly.

Related Information

None

3.4.51 ALM-303046966 MAC address flapping occurs and the interface is blocked

Description

L2IFPPI/4/MFLPIFBLOCK:OID [OID] Loop exist in vlan [INTEGER], Interface [OCTET] blocked, block-time is [GAUGE] for [OCTET], Mac Address is [OCTET].
MAC address flapping occurs and the interface is blocked.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046966	Warning	equipmentAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
INTEGER	Indicates the VLAN ID.
OCTET1	Indicates the blocked interface name.
GAUGE	Indicates the time when the interface is blocked.
OCTET3	Indicates the flapped MAC address.
OCTET2	Indicates the cause why the interface is blocked.

Impact on the System

Traffic cannot be received normally.

Possible Causes

- Cause 1: The interfaces where loops occur are added to the same VLAN.
- Cause 2: Cables are connected incorrectly.

Cause 3: Loop detection and STP are enabled to remove loops on the network.

Procedure

- Step 1** Check that cables are connected correctly. Then check whether the alarm is still reported.
- If yes, go to step 2.
 - If not, go to step 9.
- Step 2** Check whether the two interfaces that learn the same MAC address can be added to different VLANs according to the networking.
- If yes, go to step 3.
 - If not, go to step 4.
- Step 3** Modify the configuration and add the two interfaces that learn the same MAC address to different VLANs. Then check whether the alarm is still reported.
- If yes, go to step 4.
 - If not, go to step 9.
- Step 4** Check whether the ring network meets requirements.
- If yes, go to step 7.
 - If not, go to step 5.
- Step 5** Do as follows to remove loops:
1. Run the **display loop-detect eth-loop [vlan vlan-id]** command to view the blocked interface.
 2. Run the **display mac-address vlan** vlan-id command to search an interface that learns the MAC address.
 3. Shut down one interface according to the networking.
 4. Run the **reset loop-detect eth-loop vlan** vlan-id { **all** | **interface** interface-type interface-number | mac-address mac-address } command to delete the blocked interface.
- Step 6** Check whether the traffic transmission is normal.
- If yes, go to step 9.
 - If not, go to step 7.
- Step 7** Disable loop detection and enable STP. Then check whether the alarm is still reported.
- If yes, go to step 8.
 - If not, go to step 9.
- Step 8** Contact technical support personnel.
- Step 9** End.

----End

Related Information

None

3.4.52 ALM-303046965 Loop exist in vlan

Description

L2IFPPI/4/MFLPVLANALARM:OID [OID] Loop exist in vlan [INTEGER], for [OCTET].
MAC address flapping occurs.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046965	Warning	Communication alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
VLAN	Indicates the VLAN ID.
OCTET	Indicates the cause why the interface is blocked.

Impact on the System

Traffic cannot be received normally.

Possible Causes

Cause 1: The interfaces where loops occur are added to the same VLAN.

Cause 2: Cables are connected incorrectly.

Cause 3: Loop detection and STP are enabled to remove loops on the network.

Procedure

- Step 1** Check that cables are connected correctly. Then check whether the alarm is still reported.
- If yes, go to step 2.
 - If not, go to step 6.
- Step 2** Check whether the two interfaces that learn the same MAC address can be added to different VLANs according to the networking.
- If yes, go to step 3.

- If not, go to step 4.

Step 3 Modify the configuration and add the two interfaces that learn the same MAC address to different VLANs. Then check whether the alarm is still reported.

- If yes, go to step 4.
- If not, go to step 6.

Step 4 Disable loop detection and enable STP. Then check whether the alarm is still reported.

- If yes, go to step 5.
- If not, go to step 6.

Step 5 Contact technical support personnel.

Step 6 End.

----End

Related Information

None

3.4.53 ALM-303046967 MAC address learning reached the limit

Description

L2IFPPI/4/MAC_LIMIT_ALARM:OID [OID] MAC address learning reached the limit.
(L2IfIndex=[INTEGER],MacLimitVlanId=[INTEGER],
[OCTET]L2IfPortIndex=[INTEGER], BaseTrapSeverity=[INTEGER],
BaseTrapProbableCause=[INTEGER], BaseTrapEventType=[INTEGER],
MacDynAddressLearnNum=[INTEGER], MacLimitMaxMac=[INTEGER],
L2IfPortName=[OCTET])

The number of MAC addresses learned by the interface or VLAN reached the upper limit.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046967	Warning	Quality of service alarm

Parameters

Name	Meaning
[OID]	Indicates the OID of the alarm.
L2IfIndex	Indicates the interface index.

Name	Meaning
MacLimitVlanId	Indicates the VLAN ID.
L2IfPortIndex	Indicates the port index.
BaseTrapSeverity	Indicates the alarm severity.
BaseTrapProbableCause	Indicates the alarm cause.
BaseTrapEventType	Indicates the alarm type.
MacDynAddressLearnNum	Indicates the number of learned MAC addresses.
MacLimitMaxMac	Indicates the maximum number of MAC addresses to be learned.
L2IfPortName	Indicates the interface name.

Impact on the System

No more MAC addresses can be learned.

Possible Causes

The number of MAC addresses learned by the interface or VLAN reached the upper limit.

Procedure

- Step 1
Check whether the alarm is generated on an interface or in a VLAN.
- Perform one of the following operations according to networking requirements and go to step 2:
 - Increase the upper limit on the number of MAC addresses to be learned.
 - Delete unnecessary MAC addresses.
 - Ignore the alarm.
- Step 2
End.
- End

Related Information

None

3.4.54 ALM-303046929 A Port Enters the Discarding State

Description

MSTP/4/PDISC:OID [OID] The port has been set to discarding state.
(InstanceID=[INTEGER], PortInstanceID=[INTEGER], PortID=[INTEGER],
IfIndex=[INTEGER], PortName=[STRING])

The link status changed, and the port enters the Discarding state.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046929	Warning	Communication alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
InstanceID	Indicates the instance ID.
PortInstanceID	Indicates the ID of the instance to which the interface belongs.
PortID	Indicates the port ID.
IfIndex	Indicates the interface index.
PortName	Indicates the interface name.

Impact on the System

The link status changes, and the link exits the topology.

Possible Causes

1. The network topology changes that the port changes from the Forwarding state into the Discarding state.
2. A new link is added. After the topology calculation, the port enters the Discarding state.

Procedure

- Step 1** View physical devices on the network to check whether new physical connections enabled with STP are added.
- If so, go to Step 2.
 - If not, go to Step 3.

- Step 2** Check whether the added physical link is necessary.
- If so, go to Step 3.
 - If not, go to Step 4.
- Step 3** Run the **display stp [instance *instance-id*] [interface *interface-type interface-number*] [brief]** command to check whether the interfaces are consistent with the STP calculation results.
- If so, go to Step 6.
 - If not, go to Step 5.
- Step 4** Correctly deploy the network topology, and then check whether the alarm is cleared.
- If the alarm is cleared, go to Step 6.
 - If the alarm is not cleared, go to Step 3.
- Step 5** Collect alarm information and configuration information, and then contact technical support personnel.
- Step 6** End.
- End

Procedure

Check the physical devices in the network topology, whether there is a new physical link with the spanning tree protocol enabled, and check whether the newly added physical link is the required physical link.

Related Information

None

3.4.55 ALM-303046930 This Bridge Is No Longer the Root Bridge of the instance

Description

The original MSTP/2/ROOT:OID [OID]: This bridge is no longer the root bridge of the instance [instance-id].

A switch lost its status as a root bridge. Another switch with a higher priority in the network replaced it and became the root bridge.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046930	Major	Communication alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
instance-id	Indicates the instance ID.

Impact on the System

The actual network topology may not be the same as the expected one.

Possible Causes

1. A new link was added to the network topology, and the network topology changed. In addition, the newly-added device became the root bridge through the **stp root primary** command, with the MAC address smaller than that of the previous root bridge.
2. The priorities of some switches changed in the network.

Procedure

- Step 1** View physical devices on the network to check whether new physical connections enabled with STP are added.
- If so, go to Step 2.
 - If not, go to Step 4.
- Step 2** Check whether the added physical link is necessary.
- If so, go to Step 3.
 - If not, go to Step 7.
- Step 3** Run the **display stp [instance *instance-id*] [interface *interface-type interface-number*] [brief]** command to check whether the interfaces are consistent with the STP calculation results.
- If so, go to Step 9.
 - If not, go to Step 4.
- Step 4** Run the **display stp [instance *instance-id*] [interface *interface-type interface-number*] [brief]** command to check whether the priority of a bridge is changed in the network topology.
- If so, go to Step 5.
 - If not, go to Step 8.
- Step 5** Check whether the operation of changing the priority is correct.
- If so, go to Step 9.
 - If not, go to Step 6.
- Step 6** Run the **stp priority** command to re-set the priority of the local bridge as required. Alternatively, run the **undo stp priority** command or the **undo stp root**

command to restore the default value of the priority of the local bridge. Then, check whether the alarm is cleared.

- If the alarm is cleared, go to Step 9.
- If the alarm is not cleared, go to Step 8.

Step 7 Correctly deploy the network topology, and then check whether the alarm is cleared.

- If the alarm is cleared, go to Step 9.
- If the alarm is not cleared, go to Step 3.

Step 8 Collect alarm information and configuration information, and then contact technical support personnel.

Step 9 End.

----End

Related Information

None

3.4.56 ALM-303046932 The ROOT-Protection port received superior message

Description

MSTP/2/RGSUP:OID [OID] The ROOT-Protection port received superior message. (InstanceID=[INTEGER], PortInstanceID=[INTEGER], PortID=[INTEGER], IfIndex=[INTEGER], PortName=[STRING])

A switch with a higher priority outside the protection range of the root bridge attempted to become the root bridge.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046932	Major	Communication alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
InstanceID	Indicates the instance ID.
PortInstanceID	Indicates the instance ID of the port.
PortID	Indicates the port ID.

Name	Meaning
IfIndex	Indicates the interface index.
PortName	Indicates the port name.

Impact on the System

The actual network topology may not be the same as the expected one.

Possible Causes

Cause 1:

The port enabled with the root protection function received BPDUs of a higher priority than that of the bridge.

2:

The priority of some switch changed in the network.

Procedure

- Step 1** View physical devices on the network to check whether new physical connections enabled with STP are added.
- If so, go to Step 2.
 - If not, go to Step 4.
- Step 2** Check whether the added physical link is necessary.
- If so, go to Step 3.
 - If not, go to Step 7.
- Step 3** Run the **display stp [instance *instance-id*] [interface *interface-type interface-number*] [brief]** command to check whether the interfaces are consistent with the STP calculation results.
- If so, go to Step 11.
 - If not, go to Step 4.
- Step 4** Run the **display stp [instance *instance-id*] [interface *interface-type interface-number*] [brief]** command to check whether the priority of a bridge is change in the network topology.
- If so, go to Step 5.
 - If not, go to Step 8.
- Step 5** Check whether the operation of changing the priority is correct.
- If so, go to Step 8.
 - If not, go to Step 6.
- Step 6** Run the **stp priority** command to re-set the priority of the local bridge as required. Alternatively, run the **undo stp priority** command or the **undo stp root**

command to restore the default value of the priority of the local bridge. Then, check whether the alarm is cleared.

- If the alarm is cleared, go to Step 11.
- If the alarm is not cleared, go to Step 8.

Step 7 Correctly deploy the network topology, and then check whether the alarm is cleared.

- If the alarm is cleared, go to Step 11.
- If the alarm is not cleared, go to Step 8.

Step 8 Run the **display stp [instance *instance-id*] [interface *interface-type interface-number*] [brief]** command to check whether an interface under the protection of the root bridge.

- If so, go to Step 9.
- If not, go to Step 10.

Step 9 Run the **undo stp root-protection** command in the interface view to delete the configuration of the protection under the root bridge. Then, check whether the alarm is cleared.

- If the alarm is cleared, go to Step 11.
- If the alarm is not cleared, go to Step 10.

Step 10 Collect alarm information and configuration information, and then contact technical support personnel.

Step 11 End.

----End

Related Information

None

3.4.57 ALM-303046931 The edged-port that enabled BPDU-Protection will be shutdown, because it received BPDU packet

Description

MSTP/2/IVBPDU:OID [OID] The edged-port that enabled BPDU-Protection will be shutdown, because it received BPDU packet. (InstanceID=[INTEGER], PortID=[INTEGER], IfIndex=[INTEGER], PortName=[STRING])

The port enabled with BPDU protection and connected to the user received BPDUs. These BPDUs are likely to be attack packets from the user.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046931	Major	Communication alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
InstanceID	Indicates the instance ID.
PortID	Indicates the port ID.
IfIndex	Indicates the interface index.
PortName	Indicates the port name.

Impact on the System

The user network connected to this port will be broken down.

Possible Causes

The edge port received BPDUs, and BPDU protection was enabled globally.

Procedure

- Step 1** Check whether the interface should be specified as an edge port.
- If so, go to Step 2.
 - If not, go to Step 3.
- Step 2** Locate the source of the BPDUs on the interface and check whether the malicious attack exists.
- If so, go to Step 4.
 - If not, go to Step 3.
- Step 3** Run the **undo stp edged-port** command and then the **undo shutdown** command in the interface view to delete the configuration of the edge port and restart the interface. Then, check whether the alarm is cleared.
- If the alarm is cleared, go to Step 5.
 - If the alarm is not cleared, go to Step 4.
- Step 4** Collect alarm information and configuration information, and then contact technical support personnel.
- Step 5** End.
- End

Related Information

None

3.4.58 ALM-303046933 The LOOP-Protection port did not receive BPDU packets in prescriptive time

Description

MSTP/2/LGEXP:OID [OID] The LOOP-Protection port did not receive BPDU packets in prescriptive time. (InstanceID=[INTEGER], PortInstanceID=[INTEGER], PortID=[INTEGER], IfIndex=[INTEGER], PortName=[STRING])

A port enabled with loop protection failed to receive BPDUs within a specified period, and was set to be in the Discarding state.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046933	Major	Communication alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
InstanceID	Indicates the instance ID.
PortInstanceID	Indicates the instance ID of the port.
PortID	Indicates the port ID.
IfIndex	Indicates the interface index.
PortName	Indicates the port name.

Impact on the System

The interface will not forward data.

Possible Causes

1.
The peer switch did not send the BPDUs to the local switch within the specified period. The possible cause was that the spanning tree function was disabled on the peer switch.
2.
The links connected to the peer were congested. Check whether the traffic was normal.

Procedure

- Step 1** Run the **display stp [instance *instance-id*] [interface *interface-type interface-number*] [brief]** command to check whether STP is disabled on the interfaces that are directly connected.
- If so, go to Step 3.
 - If not, go to Step 2.
- Step 2** Run the **display this interface** command in the interface view to check the percentage of the rate at which the interface receives packets to the total bandwidth and then determine whether congestion occurs.
- If so, go to Step 4.
 - If not, go to Step 5.
- Step 3** Run the **stp enable** command in the interface view to enable STP. Then, check whether the alarm is cleared.
- If the alarm is cleared, go to Step 6.
 - If the alarm is not cleared, go to Step 2.
- Step 4** Repair the physical link and then check whether the alarm is cleared.
- If the alarm is cleared, go to Step 6.
 - If the alarm is not cleared, go to Step 5.
- Step 5** Collect alarm information and configuration information, and then contact technical support personnel.
- Step 6** End.
- End

Related Information

None

3.4.59 ALM-303046934 When the port receives a BPDU packet, the edged-port attribute will be disabled

Description

MSTP/4/EDGEPORT_DISABLE:OID [OID] When the port receives a BPDU packet, the edged-port attribute will be disabled. (InstanceID=[INTEGER], PortID=[INTEGER], IfIndex=[INTEGER], EdgePortEnableState=[INTEGER], PortName=[STRING])

The edge port lost the attributes of an edge port after receiving BPDUs.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046934	Warning	Communication alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
InstanceID	Indicates the instance ID.
PortID	Indicates the port ID.
IfIndex	Indicates the interface index.
EdgePortEnableState	Indicates whether BPDU-guard is enabled on the edge port.
PortName	Indicates the port name.

Impact on the System

The network topology may be changed.

Possible Causes

The edge port received BPDUs.

Procedure

Step 1 Check whether the interface should be specified as an edge port.

- If so, go to Step 2.
- If not, go to Step 3.

Step 2 Locate the source of the BPDUs on the interface and check whether the malicious attack exists.

- If so, go to Step 4.
- If not, go to Step 3.

Step 3 Run the **undo stp edged-port** and **undo shutdown** commands in the interface view to delete the configuration of the edge port and restart the interface. Then, check whether the alarm is cleared.

- If the alarm is cleared, go to Step 5.
- If the alarm is not cleared, go to Step 4.

Step 4 Collect alarm information and configuration information, and then contact technical support personnel.

Step 5 End.

----End

Related Information

None

3.4.60 ALM-303046935 The MSTP Process's Port has been set to discarding state because of detecting loopback

Description

MSTP/4/PROLBDETECTGED:OID [OID] The MSTP Process's Port has been set to discarding state because of detecting loopback. (ProcessID=[INTEGER], InstanceID=[INTEGER], PortID1=[INTEGER], PortID2=[INTEGER], PortID3=[INTEGER], PortID4=[INTEGER], PortIDFlag=[INTEGER], IfIndex=[INTEGER], PortState=[INTEGER], PortName=[STRING])

When port detected loopback, block the port and arise trap.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046935	Warning	Communication alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
ProcessID	Indicates the MSTP process ID
InstanceID	Indicates the instance ID.
PortID1	Indicates ID 1 of the port in the MSTP process.
PortID2	Indicates ID 2 of the port in the MSTP process.
PortID3	Indicates ID 3 of the port in the MSTP process.
PortID4	Indicates ID 4 of the port in the MSTP process.
PortIDFlag	Indicates the port flag.
IfIndex	Indicates the port index.
PortState	Indicates the port state.
PortName	Indicates the port name.

Impact on the System

After detecting a port blocked by local loopback, the system considers that a network storm occurs and blocks the local port to prevent the network storm from affecting services of the entire network. Services on the block port will be interrupted.

Possible Causes

When the STP port of the equipment receiving BPDU with the same designated bridge ID and designated port ID as this equipment and port, STP blocks this port and arises this trap for loopback detection will lead loop.

Procedure

- Step 1** Check whether the port where the alarm is generated is configured with local loopback.
- If so, go to Step 4.
 - If not, go to Step 2.
- Step 2** Check whether there is a loop formed by a hub and devices, one of which is connected to the port.
- If so, go to Step 5.
 - If not, go to Step 3.
- Step 3** Collect alarm information and configuration information, and then contact technical support personnel.
- Step 4** Delete the local loopback configuration to solve the problem.
- Step 5** Remove the self-loop network cable from the hub to solve the problem.
- Step 6** End.
- End

Related Information

None

3.4.61 ALM-303046695 PoE power supply is shut down

Description

POE/4/POWEROFF: OID [OID] PD powered off.(IfIndex=[INTEGER], Interface="[OCTET"])

The PD connected to the interface is powered off.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046695	Warning	equipmentAlarm

Parameters

Name	Meaning
OID	Indicates the trap ID.
IfIndex	Indicates the interface index.
Interface	Indicates the interface name.

Impact on the System

The PD connected to the interface is powered off and cannot work normally.

Possible Causes

Cause 1: The PD is removed.

Cause 2: The PD is faulty.

Cause 3: When the power is insufficient, the interface with higher priority preempts the power.

Cause 4: The interface is automatically powered off in the power-off time range.

Procedure

Step 1 Check whether the PD is removed.

- If so, go to step 2.
- If not, go to step 3.

Step 2 Install the PD and check whether the alarm is cleared.

- If so, go to step 11.
- If not, go to step 3.

Step 3 Check whether the power is sufficient.

- If so, go to step 7.
- If not, go to step 4.

Step 4 Check whether the priority of the interface is low.

- If so, go to step 5.
- If not, go to step 8.

Step 5 Check whether the interface priority is proper according to the requirements for the interface priority.

- If yes, use the **poe priority** command to re-set the interface priority.
- If not, increase the PoE power.

Step 6 Check whether the alarm is cleared.

- If so, go to step 11.
- If not, go to step 7.

Step 7 Check whether the PD is faulty.

- If so, go to step 8.
- If not, go to step 9.

Step 8 Replace the PD and check whether the alarm is cleared.

- If so, go to step 11.
- If not, go to step 9.

Step 9 Check whether the interface is in the power-off time range.

- If so, go to step 11.
- If not, go to step 10.

Step 10 Contact technical support personnel.

Step 11 End.

----End

Related Information

None

3.4.62 ALM-303046694 PoE Power Usage Exceeds the Threshold

Description

POE/4/PWRUTITHRESH: OID [OID] PSE is overdrawing power.(SlotID=[INTEGER], ConsumingPower=[INTEGER], PowerThreshold=[INTEGER])

The total PoE power consumption is greater than or equal to the alarm threshold.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046694	Warning	equipmentAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
SlotID	Indicates the ID of the slot where the alarm is generated.
ConsumingPower	Indicates the current power consumption.
PowerThreshold	Indicates the power threshold.

Impact on the System

If the alarm persists, all the PDs may be powered off because of insufficient power supply.

Possible Causes

The total power consumption of all the PDs is greater than or equal to the alarm threshold.

Procedure

- Step 1** Plan the network according to the system power supply. Increase priorities of important devices to prevent their power from being preempted. If the alarm persists, power off some PDs to ensure system reliability.

----End

Related Information

None

3.4.63 ALM-303046728 After server detection is enabled and the alarm action is configured, the device detects that the Portal server changes from Down to Up

Description

WEB/4/PortalServerUp:OID [OID] The portal server is up. (IP:[IPADDR], Vpn-Instance:[OCTET])

After server detection is enabled and the alarm action is configured, the device detects that the Portal server changes from Down to Up.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046728	Warning	equipmentAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
IP	Indicates the IP address of the Portal server.

Impact on the System

None

Possible Causes

The Portal server changes from Down to Up.

Procedure

Step 1 This log is informational only, and no action is required.

----End

Related Information

None

3.4.64 ALM-303046729 After server detection is enabled and the alarm action is configured, the device detects that the Portal server changes from Up to Down

Description

WEB/4/PortalServerDown warning:OID [OID] The portal server is down. (IP: [IPADDR], Vpn-Instance:[OCTET])

After server detection is enabled and the alarm action is configured, the device detects that the Portal server changes from Up to Down.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046729	Warning	equipmentAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
IP	Indicates the IP address of the Portal server.

Impact on the System

The Portal authentication function does not work.

Possible Causes

The Portal server changes from Up to Down.

Procedure

Step 1 Check whether the Portal server can work properly and whether the Portal service can be used properly.

- If the Portal server works properly, check the network connectivity between the Portal server and device. If the network connection is disconnected, restore the network connection.
- If the Portal server cannot work properly, restore the Portal server to the normal state.

----End

Related Information

None

3.4.65 ALM-303046730 The number of online Portal users exceeded the upper alarm threshold

Description

WEB/4/PORTALMaxUserAlarm: OID [OID] The number of portal users reached the maximum.(Slot:[OCTET] User-num:[INTEGER] Threshold:[INTEGER]%)

The number of online Portal users exceeded the upper alarm threshold.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046730	Warning	equipmentAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
Slot	Indicates a slot ID on a device.
User-num	Indicates the maximum number of Portal authentication users allowed on the device.
Threshold	Indicates the upper alarm threshold on the percentage of online Portal authentication user count against the maximum number of Portal authentication users allowed on the device.

Impact on the System

None

Possible Causes

The number of online Portal users exceeded the upper alarm threshold.

Procedure

- Step 1** Run the **display this** command in the system view to check whether the upper alarm threshold configured by the **portal user-alarm percentage** command is proper.
- If so, go to step 2.
 - If not, modify the upper alarm threshold.
- Step 2** Run the **display portal** command to check whether the maximum number of Portal authentication users allowed on the device is proper.
- If so, go to step 3.
 - If not, run the **portal max-user** command to modify the maximum number of Portal authentication users.
- Step 3** Run the **display access-user** command to check whether online Portal authentication users are proper.

- If so, replace the device with a higher-performance device.
- If not, replan the network.

Step 4 Collect log and configuration information, and contact technical support personnel.

----End

3.4.66 ALM-303046731 The number of online Portal users was equal to or smaller than the lower alarm threshold

Description

WEB/4/PORTALUserClearAlarm: OID [OID] The Portal Max User Alarm is cleared.
(Slot:[OCTET] User-num:[INTEGER] Threshold:[INTEGER]%)

The number of online Portal users was equal to or smaller than the lower alarm threshold.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046731	Warning	equipmentAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
Slot	Indicates a slot ID on a device.
User-num	Indicates the maximum number of Portal authentication users allowed on the device.
Threshold	Indicates the lower alarm threshold on the percentage of online Portal authentication user count against the maximum number of Portal authentication users allowed on the device.

Impact on the System

None

Possible Causes

The number of online Portal users was equal to or smaller than the lower alarm threshold.

Procedure

Step 1 This log message is informational only, and no action is required.

----End

Related Information

None

3.4.67 ALM-303046921 The number of public IPv4 prefixes exceeded the maximum value

Description

RM/2/PUBLIC_IPV4_PREFIX_EXCEED:OID [OID] The number of public IPv4 prefixes exceeded the maximum value. (PrefixCount=[Integer], MaxValue=[Integer])

The number of IPv4 public route prefixes exceeded that supported by the system.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046921	Major	Quality of service alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
PrefixCount	Indicates the number of IPv4 public route prefixes in the routing table.
MaxValue	Indicates the maximum number of IPv4 public route prefixes supported by the device.

Impact on the System

New IPv4 public route prefixes cannot be added to the routing table. Services will be affected if the number of IPv4 route prefixes keeps increasing.

Possible Causes

Cause 1:

A large number of IPv4 dynamic protocol routes (BGP or IGP routes for example), static routes, direct routes, or UNR routes were added to the routing table.

Cause 2:

The maximum number of IPv4 public route prefixes supported by the system was decreased.

Procedure

Step 1 Run the **display ip routing-table statistics** command to check the number of IPv4 public route prefixes and the number of routes of each protocol that are added to the routing table.

Check whether services need these routes or whether the routes are added to the routing table due to incorrect configurations.

- If the routes are added to the routing table due to incorrect configurations, go to [Step 2](#).
- If services need these routes, replace the license or contact technical support personnel for specification expansion.

Step 2 Adjust the configurations to delete unneeded routes, and check whether the RM_1.3.6.1.4.1.2011.5.25.145.19.1.2 hwPublicIpv4PrefixExceedClear alarm is generated.

- If the RM_1.3.6.1.4.1.2011.5.25.145.19.1.2 hwPublicIpv4PrefixExceedClear alarm is not generated, go to [Step 3](#).
- If the RM_1.3.6.1.4.1.2011.5.25.145.19.1.2 hwPublicIpv4PrefixExceedClear alarm is generated, go to [Step 4](#).

Step 3 Collect alarm information and configuration information, and then contact technical support personnel.

Step 4 End.

----End

Related Information

None

3.4.68 ALM-303046936 Attack occurred

Description

SECE/4/STRACKUSER: OID=[OID] Attack occurred.(Interface=[STRING], SourceMAC=[STRING], CVLAN=[ULONG], PVLAN=[ULONG], EndTime=[STRING], TotalPackets=[ULONG])

The system detects an attack.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046936	Warning	securityServiceOrMechanismViolation

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
Interface	Indicates the access interface of the attacker.
SourceMAC	Indicates the Source MAC address of packets sent from the attacker.
BCVLAN	Indicates the maximum rate of broadcast packets.
PVLAN	Indicates the inner VLAN ID of packets sent from the attacker.
EndTime	Indicates the end time of the attack.
TotalPackets	Indicates the number of packets received from the attacker.

Impact on the System

The CPU is busy processing attack packets. As a result, normal service packets cannot be processed in time or even discarded.

Possible Causes

The rate of packets with the specified MAC address and VLAN ID sent to the CPU exceeds the alarm threshold.

Procedure

- Step 1
If the user initiates the attack, you can set the action taken on attack packets to deny, or configure a traffic policy to discard attack packets.
- Step 2
If the fault cause is unknown, collect device configurations, alarms, and logs, and then contact technical support personnel.
- Step 3
End.
- End

Related Information

None

3.4.69 ALM-303046937 Attack occurred

Description

SECE/4/STRACKPORT: OID=[OID] Attack occurred.(Interface=[STRING], CVLAN=[ULONG], PVLAN=[ULONG], EndTime=[STRING], TotalPackets=[ULONG])

The system detects an attack on an interface.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046937	Warning	securityServiceOrMechanismViolation

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
Interface	Indicates the access interface of the attacker.
CVLAN	Indicates the outer VLAN ID of the attacker.
PVLAN	Indicates the inner VLAN ID of packets sent from the attacker.
EndTime	Indicates the end time of the attack.
TotalPackets	Indicates the number of packets received from the attacker.

Impact on the System

The CPU is busy processing attack packets. As a result, normal service packets cannot be processed in time or even discarded.

Possible Causes

The number of packets with the specified interface and VLAN ID sent to the CPU exceeds the alarm threshold.

Procedure

- Step 1** If an attack is initiated by a user and the user is the only one connected to the interface, you can shut down the interface and check whether the interface is normal.
- Step 2** If the interface is connected to multiple users and some users initiate attacks, you can set the action taken on attack packets to deny, or configure a traffic policy to discard attack packets.
- Step 3** If only entries exist on the interface or entries cannot be determined, collect device configurations, alarms, and logs, and then contact technical support personnel.
- Step 4** End.
- End

Related Information

None

3.4.70 ALM-303046944 Gateway Conflict

Description

SECE/4/GATEWAY_CONFLICT:OID=[OID] Gateway conflict.
(SourceInterface=[OCTET], SourceIP=[OCTET], SourceMAC=[OCTET],
PVLAN=[INTEGER], CVLAN=[INTEGER])

The system detects attack packets whose source IP addresses are the same as the gateway IP address.



NOTE

Only the AC6605 supports this alarm.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046944	Warning	equipmentAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
SourceInterface	Indicates the source interface of packets.

Name	Meaning
SourceIP	Indicates the source IP address of packets.
SourceMAC	Indicates the source MAC address of packets.
PVLAN	Indicates the outer VLAN ID of packets.
CVLAN	Indicates the inner VLAN ID of packets.

Impact on the System

If this alarm is generated, the user gateway information may be modified by an attacker. As a result, the user is attacked and user services are interrupted.

Possible Causes

The device is attacked by packets whose source IP address is the same as the gateway IP address.

Procedure

- Step 1** Find the interface where the gateway conflict occurs according to the value of **SourceInterface**.
- Step 2** Lock the user who sends gateway conflict packets according to the values of **SourceMAC** and **PVLAN**.
- Step 3** Check whether the allocated address of the user conflicts with the gateway address. If the address conflicts, allocate an address to the user again. If the address does not conflict, the user may be the attacker. In this case, you can take such measures as disconnecting the user.

----End

Related Information

None

3.4.71 ALM-303046945 ARP Entry Attack

Description

SECE/4/ARP_ENTRY_CHECK:OID=[OID] Arp entry attack.(SourceInterface=[OCTET], SourceIP=[OCTET], SourceMAC=[OCTET], PVLAN=[INTEGER], CVLAN=[INTEGER])

The system detects attack packets used to modify ARP entries.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046945	Warning	equipmentAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
SourceInterface	Indicates the source interface of packets.
SourceIP	Indicates the source IP address of packets.
SourceMAC	Indicates the source MAC address of packets.
PVLAN	Indicates the outer VLAN ID of packets.
CVLAN	Indicates the inner VLAN ID of packets.

Impact on the System

If this alarm is generated, ARP entries on the AC may be changed to ARP entries of attackers. As a result, user traffic is intercepted by attackers and user services are interrupted.

Possible Causes

The AC is attacked by packets used to modify ARP entries.

Procedure

- Step 1** Find the interface where attacks occur according to **SourceInterface**.
- Step 2** Check whether users who are not in the DHCP snooping binding table range are connected to the interface.
- Step 3** If new users are connected, run related DHCP snooping commands to generate the DHCP snooping binding table. Then find the interface where the gateway conflict occurs according to the value of **SourceInterface**.

----End

Related Information

None

3.4.72 ALM-303046946 Invalid Packet

Description

SECE/4/ARP_PACKET_CHECK:OID=[OID] Invalid packet.(SourceInterface=[OCTET], SourceIP=[OCTET], SourceMAC=[OCTET], PVLAN=[INTEGER], CVLAN=[INTEGER])

The system detects invalid ARP packets.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046946	Warning	equipmentAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
SourceInterface	Indicates the source interface of packets.
SourceIP	Indicates the source IP address of packets.
SourceMAC	Indicates the source MAC address of packets.
PVLAN	Indicates the outer VLAN ID of packets.
CVLAN	Indicates the inner VLAN ID of packets.

Impact on the System

If this alarm is generated, the AC may be attacked. If the attack traffic volume is heavy, the AC is busy processing attack packets. As a result, services of authorized users are interrupted.

Possible Causes

The AC receives invalid ARP packets.

Procedure

- Step 1** Find the interface where the gateway conflict occurs according to the value of **SourceInterface**.

- Step 2** Lock the user who sends gateway conflict packets according to the values of **SourceMAC** and **PVLAN**.
- Step 3** Check whether the allocated address of the user conflicts with the gateway address. If the address conflicts, allocate an address to the user again. If the address does not conflict, the user may be the attacker. In this case, you can take such measures as disconnecting the user.
- End

Related Information

None

3.4.73 ALM-303046947 The Number of Packets Discarded by DAI Reaches the Threshold

Description

SECE/4/DAI_DROP_ALARM:OID=[OID] The packet number dropped by DAI reaches [INTEGER1], exceeds the alarm threshold [INTEGER2],Interface=[OCTET].

The number of packets discarded by Dynamic ARP Inspection (DAI) exceeds the alarm threshold.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046947	Warning	equipmentAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
INTEGER1	Indicates the number of discarded packets.
INTEGER2	Indicates the alarm threshold.
Interface	Indicates the source interface of packets.

Impact on the System

If this alarm is generated, the AC may be attacked. If the attack traffic volume is heavy, the AC is busy processing attack packets. As a result, services of authorized users are interrupted.

Possible Causes

The number of packets discarded by DAI exceeds the alarm threshold.

Procedure

Step 1 This alarm is informational and no action is required.

----End

Related Information

None

3.4.74 ALM-303046948 The Rate of ARP Packets Exceeds the Alarm Threshold

Description

SECE/4/ARP_GLOBAL_SPEEDLIMIT_ALARM:OID=[OID] The global arp packet speed exceeds the speed-limit value [INTEGER].

The rate of ARP packets exceeds the alarm threshold.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046948	Warning	equipmentAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
INTEGER	Indicates the alarm threshold.

Impact on the System

If the alarm is generated, it indicates that the user traffic volume exceeds the threshold. The excess traffic is discarded by the AC. As a result, user traffic may be interrupted intermittently.

Possible Causes

The global ARP packet rate exceeds the alarm threshold.

Procedure

Step 1 This alarm is informational and no action is required.

----End

Related Information

None

3.4.75 ALM-303046949 The Interface ARP Packet Speed Exceeds the Speed-limit Value

Description

SECE/4/ARP_IF_SPEEDLIMIT_ALARM:OID=[OID] The interface arp packet speed exceeds the speed-limit value [INTEGER], interface=[OCTET].

The rate of ARP packets on an interface exceeds the alarm threshold.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046949	Warning	equipmentAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
INTEGER	Indicates the alarm threshold.
Interface	Indicates the source interface of packets.

Impact on the System

If the alarm is generated, it indicates that the user traffic volume exceeds the threshold. The excess traffic is discarded by the AC. As a result, user traffic may be interrupted intermittently.

Possible Causes

The rate of ARP packets on an interface exceeds the alarm threshold.

Procedure

Step 1 This alarm is informational and no action is required.

----End

Related Information

None

3.4.76 ALM-303046950 The Rate of ARP Miss Packets Exceeds the Alarm Threshold

Description

SECE/4/ARPMISS_GLOBAL_SPEEDLIMIT_ALARM:OID=[OID] The global arp-miss packet speed exceeds the speed-limit value [INTEGER].

The rate of ARP Miss packets of the system exceeds the alarm threshold.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046950	Warning	equipmentAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
INTEGER	Indicates the alarm threshold.

Impact on the System

If the alarm is generated, it indicates that the user traffic volume exceeds the threshold. The excess traffic is discarded by the AC. As a result, user traffic may be interrupted intermittently.

Possible Causes

The rate of ARP Miss packets of the system exceeds the alarm threshold.

Procedure

Step 1 This alarm is informational and no action is required.

----End

Related Information

None

3.4.77 ALM-303046951 The Rate of ICMP Packet Exceeds the Threshold

Description

SECE/4/ICMP_GLOBAL_SPEEDLIMIT_ALARM:OID=[OID]. Global icmp packet speed exceeds the speed-limit value [INTEGER].

The rate of ICMP packets exceeds the alarm threshold.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046951	Warning	equipmentAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
INTEGER1	Indicates the alarm threshold.

Impact on the System

If the alarm is generated, it indicates that the user traffic volume exceeds the threshold. The excess traffic is discarded by the AC. As a result, user traffic may be interrupted intermittently.

Possible Causes

The global ICMP packet rate exceeds the alarm threshold.

Procedure

Step 1 This alarm is informational and no action is required.

----End

Related Information

None

3.4.78 ALM-303046952 The Rate of ICMP Packets on an Interface Exceeds the Alarm Threshold

Description

SECE/4/ICMP_IF_SPEEDLIMIT_ALARM:OID=[OID]. Interface icmp packet speed exceed the speed-limit value [INTEGER],Interface=[OCTET].

The rate of ICMP packets on an interface exceeds the alarm threshold.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046952	Warning	equipmentAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
INTEGER1	Indicates the alarm threshold.
Interface	Indicates the source interface of packets.

Impact on the System

If the alarm is generated, it indicates that the user traffic volume exceeds the threshold. The excess traffic is discarded by the AC. As a result, user traffic may be interrupted intermittently.

Possible Causes

The rate of ICMP packets on an interface exceeds the alarm threshold.

Procedure

Step 1 This alarm is informational and no action is required.

----End

Related Information

None

3.4.79 ALM-303046697 The AP Is Cold Restarted

Description

SNMP/4/COLDSTART:OID [OID] coldStart.

The device was cold started.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046697	Minor	equipmentAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.

Impact on the System

The alarm, generated because of the device cold start, brings no adverse impact on the system.

Possible Causes

The device was cold started.

Procedure

- This trap message is informational only, and no action is required.

Related Information

None

3.4.80 ALM-303046696 The AP Is Hot Restarted

Description

SNMP/4/WARMSTART:OID [OID] warmStart.

The device was hot started, or the SNMP agent was enabled.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046696	Minor	equipmentAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.

Impact on the System

The alarm, generated because of the device warm start, brings no adverse impact on the system.

Possible Causes

- The device was hot started.
- The SNMP agent was enabled.

Procedure

- This trap message is informational only, and no action is required.

Related Information

None

3.4.81 ALM-303046953 MD5 Authentication Failed

Description

SOCKET/4/TCP_MD5_FAIL:OID [OID] MD5 authentication failed.
(SourceAddress=[IPADDR], SourcePort=[INTEGER], ForeignAddress=[IPADDR], ForeignPort=[INTEGER], Protocol=[OCTET], VrfName=[OCTET])

The MD5 authentication of the TCP connection failed.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046953	Warning	Communication alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
SourceAddress	Indicates the local IP address of the TCP connection.
SourcePort	Indicates the local port number.
ForeignAddress	Indicates the destination IP address of the TCP connection.
ForeignPort	Indicates the destination port number.
Protocol	Indicates the name of the upper layer protocol.
VrfName	Indicates the VRF name.

Impact on the System

The TCP connection cannot be set up normally and upper layer protocols such as LDP and BGP cannot set up sessions.

Possible Causes

- 1: The MD5 authentication passwords on the two ends of the TCP connection were inconsistent.
- 2: Only one end of the TCP connection was configured with the MD5 authentication password.

Procedure

- Run the **display current-configuration** command on the devices at the two ends of the TCP connection to check whether the devices are configured with MD5 authentication passwords.
 - Only one device is configured with the MD5 authentication password. Configure the MD5 authentication password for the other devices and ensure that the MD5 authentication passwords on the two devices must be the same, and then go to Step 3.
 - If the two devices are configured with MD5 authentication passwords but the passwords are different, go to Step 2.
- Reconfigure the MD5 authentication passwords to make the MD5 authentication passwords consistent on the two ends of the TCP connection, and then go to Step 3.
- Check whether the MD5 authentication is successful.
 - If so, go to Step 4.
 - If not, go to Step 5.

- Collect alarm information and configuration information, and then contact technical support personnel.
- End.

Related Information

None

3.4.82 ALM-3416067 Abnormal Cable SNR

Description

WLAN/4/SNR_ABNORMAL:OID [OID] The current network cable quality is poor, causing packet loss risks.(APMAC=[OPAQUE], APName=[STRING], InterfaceIndex=[INTEGER], InterfaceName=[OCTET], APID=[INTEGER])

The network cable quality is poor and packet loss may occur.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3416067	Warning	Communication alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
APMAC	MAC address of an AP.
APName	AP name.
InterfaceIndex	Interface index.
InterfaceName	Interface name.
APID	AP ID.

Impact on the System

The network cable quality is poor and packet loss may occur.

Possible Causes

When the MultiGE electrical interface works at the rate of 2.5 Gbit/s or higher, the network cable quality is poor or signal interference exists.

Procedure

- Replace the network cable with a high-quality network cable.
- Contact technical support personnel.

3.4.83 ALM-303046403 The Port Is Down, Resulting In A Failure to Detect the Network Cable Quality

Description

WLAN/4/SNR_DETECT_NOTSUPPORT:OID [OID] The port is Down, resulting in a failure to detect the network cable quality. (InterfaceIndex=[INTEGER], InterfaceName=[OCTET])

The network cable quality cannot be checked.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046403	Warning	Communication alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
InterfaceIndex	Interface index.
InterfaceName	Interface name.

Impact on the System

None

Possible Causes

The MultiGE electrical interface changes from Up to Down.

Procedure

- This alarm is informational only and no action is required.

3.4.84 ALM-303046791 An AP Changes to Fault

Description

WLAN/2/AP_FAULT:OID [OID] AP changes to fault. (APMAC=[OPAQUE], APTYPE=[STRING], APName=[STRING], APFAULTTIME=[INTEGER], APID=[INTEGER])

An RU goes offline.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046791	Major	equipmentAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
APMAC	Indicates the MAC address of an AP.
APType	Indicates the AP type.
APName	Indicates the AP name.
APFAULTTIME	Indicates the number of times the AP goes offline.
APID	Indicates the AP ID.

Impact on the System

The AC cannot manage the AP, and the AP-related services cannot work properly.

Possible Causes

- Cause 1: The AP is disconnected from the AC.
- Cause 2: The AP is powered off.
- Cause 3: The heartbeat packets between AP and AC are lost.
- Cause 4: The AC licenses are insufficient.
- Cause 5: The AC and AP versions do not match.

Procedure

- Step 1** Check whether the AP is disconnected from the AC.
- If so, connect them.
 - If not, go to Step 2.
- Step 2** Check whether the AP is powered off.
- If so, power on the AP.
 - If not, go to Step 3.
- Step 3** Check whether the AP and AC can exchange heartbeat packets.
- If not, verify network connectivity.
 - If so and the alarm still exists, go to Step 4.
- Step 4** Run the **display license resource usage** command to check whether AC licenses are sufficient.
- If so, go to Step 5.
 - If not, apply for more AC licenses.
- Step 5** Run the **display ap all** command to check whether the AC and AP versions match.
- If so, go to Step 6.
 - If not, upgrade the AC and AP to matching versions.
- Step 6** Collect alarm messages, log messages, and configurations, and then contact the technical support personnel.
- Step 7** End.
- End

Related Information

None

3.4.85 ALM-303046792 AP Ping Result

Description

WLAN/4/AP_PING_RESULT:OID [OID] AP ping result. (APMAC=[OPAQUE], APType=[STRING], APName=[STRING], SuccessCount=[INTEGER], FailureCount=[INTEGER]. AverageResponseTime=[INTEGER]ms, MinimumResponseTime=[INTEGER]ms, MaximumResponseTime=[INTEGER]ms, APID=[INTEGER])

The result of AP ping operations issued from the NMS to the AP is reported.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046792	Warning	other

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
APMAC	Indicates the MAC address of an AP.
APType	Indicates the AP type.
APName	Indicates the AP name.
SuccessCount	Indicates whether the latest AP ping operation succeeds and the number of successful ping operations. Only the result of the latest ping is kept.
FailureCount	Indicates whether the latest AP ping operation succeeds and the number of failed ping operations. Only the result of the latest ping is kept.
AverageResponseTime	Indicates the average response time when you query the result of an AP ping operation. The unit is milliseconds. Only the result of the latest ping is kept.
MinimumResponseTime	Indicates the minimum response time when you query the result of an AP ping operation. The unit is milliseconds. Only the result of the latest ping is kept.
MaximumResponseTime	Indicates the maximum response time when you query the result of an AP ping operation. The unit is milliseconds. Only the result of the latest ping is kept.
APID	Indicates the AP ID.

Impact on the System

None

Possible Causes

The AP ping operation issued from the NMS to the AP is finished.

Procedure

Step 1 This alarm is informational only, and no action is required.

----End

Related Information

None

3.4.86 ALM-303046793 AP Is Committed Over

Description

WLAN/4/AP_COMMIT_OVER:OID [OID] AP is committed over.
(APMAC=[OPAQUE], APName=[STRING], APID=[INTEGER])

The AP configuration was committed.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046793	Warning	equipmentAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
APMAC	Indicates the MAC address of an AP.
APName	Indicates the AP name.
APID	Indicates the AP ID.

Impact on the System

None

Possible Causes

None

Procedure

Step 1 This alarm is informational only, and no action is required.

----End

Related Information

None

3.4.87 ALM-303046795 Unauthorized AP Record Exists

Description

WLAN/4/UNAUTHORIZED_AP_RECORD_EXIST:OID [OID] Unauthorized AP record exists.(Record number=[INTEGER])

An unauthorized AP alarm exists.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046795	Warning	equipmentAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
Record number	Indicates the number of APs failing authentication.

Impact on the System

Rogue APs occupy links.

Possible Causes

Cause 1: The AP authentication mode is set to MAC address authentication, but the AP is not added offline and its MAC address is not in the whitelist.

Cause 2: The AP authentication mode is set to SN authentication, but the AP is not added offline and its SN is not in the whitelist.

Procedure

- Step 1** Add authorized APs to the whitelist (add SNs or MAC addresses to the whitelist according to the AP authentication mode). Then, check whether the alarm persists.
- If so, go to Step 2.
 - If not, go to Step 3.

- Step 2** Collect alarm messages, log messages, and configurations, and then contact the technical support personnel.
- Step 3** End.
- End

Related Information

3.4.88 ALM-303046798 AP CPU Overload Notify

3.4.88 ALM-303046798 AP CPU Overload Notify

Description

WLAN/4/AP_CPU_OVERLOAD: OID [OID] AP CPU overload notify.
(APMAC=[OPAQUE], APName=[STRING], ApCpuRate=[INTEGER], the top three thread CPU occupancy are [STRING], APID=[INTEGER])

The AP's CPU usage exceeds the upper threshold.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046798	Warning	equipmentAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object of the alarm.
APMAC	Indicates the AP's MAC address.
APName	Indicates the AP name.
ApCpuRate	Indicates the AP's CPU usage.
[STRING2]	Indicates the top 3 threads with the highest CPU usage.
APID	Indicates the AP ID.

Impact on the System

The CPU usage exceeds the upper threshold. If the threshold is not high (for example, 50% or 60%), services are not affected. If the threshold is high (for example 90%), the AP reports the alarm, and packet loss may occur on the AP or the AP may be disconnected.

Possible Causes

Cause 1: The alarm threshold of the CPU usage is low.

Cause 2: The device provides too many services.

Cause 3: The device is attacked, causing high CPU usage.

Procedure

- Step 1** Run the **display ap-system-profile** command to check the alarm threshold for AP's CPU usage. Check whether the alarm threshold is set properly.
1. If so, go to [Step 3](#).
 2. If not, go to [Step 2](#).
- Step 2** Run the **cpu-usage threshold** command to set a proper alarm threshold for CPU usage. After that, check whether the alarm persists.
1. If this alarm persists, go to [Step 3](#).
 2. If the alarm is cleared, go to [Step 6](#).
- Step 3** Check whether the traffic volume is high. For example, check whether STAs frequently roam or a large number of STAs frequently go online or offline and check that the system runs normally.
1. If the traffic volume is high and the system runs normally, ignore the alarm.
 2. If the traffic volume is low, go to [Step 4](#).
- Step 4** Log in to the AP and run the **display cpu-usage** command in the diagnostic view to check the CPU usage of each task. Locate tasks with high CPU usage and delete unnecessary services or configurations to reduce the CPU usage.
1. If the alarm persists after some services are deleted, go to [Step 5](#).
 2. If the alarm is cleared, go to [Step 6](#).
- Step 5** Collect trap, log, and configuration information, as well as the CPU usage information in [Step 4](#), and contact technical support personnel.
- Step 6** If the alarm is cleared, no further action is required.

----End

Related Information

None

3.4.89 ALM-303046799 The Memory Usage of an AP Exceeds the Upper Threshold

Description

WLAN/4/AP_MEM_OVERLOAD: OID [OID] AP memory overload notify.
(APMAC=[OPAQUE], APName=[STRING], ApMemRate=[INTEGER],
APID=[INTEGER])

The AP's memory usage exceeds the upper threshold.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046799	Warning	equipmentAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object of the alarm.
APMAC	Indicates the AP's MAC address.
APName	Indicates the AP name.
ApMemRate	Indicates the AP's memory usage.
APID	Indicates the AP ID.

Impact on the System

The memory usage exceeds the upper threshold. If the threshold is not high (for example, 50% or 60%), services are not affected. If the threshold is high (for example 90%), the AP reports the alarm, and packet loss may occur on the AP or the AP may be disconnected.

Possible Causes

Cause 1: The memory alarm threshold is low.

Cause 2: The device provides too many services.

Procedure

- Step 1** Run the **display ap-system-profile** command to check the alarm threshold for memory usage. Check whether the alarm threshold is set properly.
- If so, go to step 3.
 - If not, go to step 2.
- Step 2** Run the **memory-usage threshold** command to set a proper alarm threshold for memory usage. After that, check whether the alarm persists.
- If the alarm persists, go to step 3.
 - If the alarm is cleared, go to step 5.
- Step 3** 3. Delete unnecessary services and configurations to reduce memory usage. Then check whether the alarm is cleared.
- If the alarm persists, go to step 4.
 - If the alarm is cleared, go to step 5.

- Step 4** Collect alarms, logs, and configurations, and then contact technical support personnel.
- Step 5** End.
- End

Related Information

None

3.4.90 ALM-303046693 No STA Can Be Associated with the AP

Description

WLAN/4/AP_REACH_MAX_USERS:OID [OID] AP has the max number of stations notify.(APMAC=[OPAQUE], APName=[STRING], FailCause=[INTEGER], PermitNum=[INTEGER], APID=[INTEGER])

The maximum number of STAs associated with the AP was reached.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046693	Warning	equipmentAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
APMAC	Indicates the MAC address of an AP.
APName	Indicates the AP name.
FailCause	Indicates the cause for the STA authentication failure.
PermitNum	Indicates the maximum number of STAs that can be associated with the AP.
APID	Indicates the AP ID.

Impact on the System

The newly added STAs cannot go online.

Possible Causes

The number of STAs connected to an AP has reached the upper limit. New STAs cannot connect to the VAP.

Procedure

Step 1 Re-plan the network and increase the network capacity.

----End

Related Information

None

3.4.91 ALM-303046801 AC Has System Switched Notify

Description

WLAN/4/AC_SYSTEM_SWITCH: OID [OID] AC has system switched notify.
(APMAC=[OPAQUE], APName=[STRING], APSN=[OCTET], SwitchType=[INTEGER], APID=[INTEGER])

The active/standby switchover occurred on the AC.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046801	Warning	equipmentAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
APMAC	Indicates the MAC address of an AP.
APName	Indicates the AP name.
APSN	Indicates the sequence number of an AP.
SwitchType	Indicates the switchover type of the AC.
APID	Indicates the AP ID.

Impact on the System

None

Possible Causes

The AC that is connected to the AP is faulty, or the network becomes unstable.

Procedure

- Step 1

Check the running status of the AC, which manages APs before the switchover.
 - If the AC is reset, go to Step 4.
 - If the AC is not reset, go to Step 2.
- Step 2

Check whether the network is attacked or congested.
 - If so, go to Step 3.
 - If not, go to Step 4.
- Step 3

Analyze the cause for network instability and rectify the fault based on the actual network situation.
- Step 4

Collect alarm messages, log messages, and configurations, and then contact the technical support personnel.
- Step 5

End.

----End

Related Information

None

3.4.92 ALM-303046800 Dying Gasp Notify

Description

WLAN/4/AP_DYING_GASP: OID [OID] Dying gasp notify.(APMAC=[OPAQUE], APName=[STRING], APID=[INTEGER])

The dying gasp alarm was generated.

NOTE

This alarm is not supported by the AP4051TN, AP6052DN, AP7052DN, AP7152DN, AP7052DE, AP8050TN-HD, AP8082DN, or AP8182DN.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046800	Warning	equipmentAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
APMAC	Indicates the MAC address of an AP.
APName	Indicates the AP name.
APID	Indicates the AP ID.

Impact on the System

The AP cannot work properly.

Possible Causes

The AP is powered off or its power supply is unstable.

Procedure

- Step 1** Check whether the power supply for the AP is normal.
- If the AP is powered off, go to Step 2.
 - If the power supply is working properly, go to Step 3.
- Step 2** Power on the power supply. Then, check whether the alarm persists.
- If so, go to Step 3.
 - If not, go to Step 6.
- Step 3** Check whether the AP's power supply is stable.
- If so, go to Step 4.
 - If not, go to Step 6.
- Step 4** Provide stable power supply to the AP. Then, check whether the alarm persists.
- If so, go to Step 5.
 - If not, go to Step 6.
- Step 5** Collect alarm messages, log messages, and configurations, and then contact the technical support personnel.
- Step 6** End.

----End

Related Information

None

3.4.93 ALM-303046797 The AP's Temperature Is Too Low

Description

WLAN/4/AP_TEMPERATURE_TOO_LOW:OID [OID] The AP's temperature is too low. (APMAC=[OPAQUE], APName=[STRING], Temperature=[INTEGER]°C, APID=[INTEGER])

The AP's temperature is lower than the lower temperature threshold.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046797	Warning	equipmentAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
APMAC	Indicates the MAC address of an AP.
APName	Indicates the AP name.
Temperature	Indicates the temperature of the AP.
APID	Indicates the AP ID.

Impact on the System

The AP's temperature is lower than the lower temperature threshold.

- If the lower temperature threshold is not low, the low AP temperature has no impact on services.
- If the lower temperature threshold is low, the AP cannot work properly, affecting WLAN services.

Possible Causes

Cause 1: The lower temperature threshold is set to an improper value.

Cause 2: The ambient temperature is too low.

Procedure

- Step 1** Run the **display ap-system-profile { all | name *profile-name* }** command to check whether the lower temperature threshold is set properly.

- If so, go to Step 3.
- If not, go to Step 2.

Step 2 Run the **low-temperature threshold** *min-temperature* command to set a proper lower temperature threshold.

- If the alarm persists, go to Step 3.
- If the alarm is cleared, go to Step 5.

Step 3 Increase the ambient temperature by turning up air-conditioners.

- If the alarm persists, go to Step 4.
- If the alarm is cleared, go to Step 5.

Step 4 Collect alarm messages, log messages, and configurations, and then contact the technical support personnel.

Step 5 End.

----End

Related Information

3.4.94 ALM-303046796 The AP's Temperature Is Too High

3.4.94 ALM-303046796 The AP's Temperature Is Too High

Description

WLAN/4/AP_TEMPERATURE_TOO_HIGH:OID [OID] The AP's temperature is too high. (APMAC=[OPAQUE], APName=[STRING], Temperature=[INTEGER]°C, APID=[INTEGER])

The AP's temperature is higher than the upper temperature threshold.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046796	Warning	equipmentAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
APMAC	Indicates the MAC address of an AP.
APName	Indicates the AP name.

Name	Meaning
Temperature	Indicates the temperature of the AP. NOTE When the alarm is triggered on the R240D, R250D-E, AP2030DN, AP2050DN, AP2050DN-E, AP4030DN, AP4050DN, AP4050DN-S, AP4051DN, AP4151DN, AP1050DN-S, AP2051DN, AP2051DN-E, R251D-E and AP4130DN, the Temperature parameter indicates the alarm triggering threshold rather than the AP's actual temperature.
APID	Indicates the AP ID.

Impact on the System

The AP's temperature is higher than the upper temperature threshold.

- If the upper temperature threshold is not high, it has no impact on services.
- If the upper temperature threshold is high, the AP cannot work properly, affecting WLAN services.

Possible Causes

Cause 1: The upper temperature threshold is set to an improper value.

Cause 2: The ambient temperature is high.

Procedure

- Step 1** Run the **display ap-system-profile { all | name *profile-name* }** command to check whether the upper temperature threshold is set properly.
- If so, go to Step 3.
 - If not, go to Step 2.
- Step 2** Run the **high-temperature threshold *max-temperature*** command to set a proper upper temperature threshold.
- If the alarm persists, go to Step 3.
 - If the alarm is cleared, go to Step 5.
- Step 3** Reduce the ambient temperature by turning down air-conditioners or increase heat dissipation devices.
- If the alarm persists, go to Step 4.
 - If the alarm is cleared, go to Step 5.
- Step 4** Collect alarm messages, log messages, and configurations, and then contact the technical support personnel.
- Step 5** End.
- End

Related Information

3.4.93 ALM-303046797 The AP's Temperature Is Too Low

3.4.95 ALM-303046803 AP Optical Module Received Power Is Too Low Notify

Description

WLAN/4/AP_OPTICAL_RX_POWER_TOO_LOW:OID [OID] AP optical module received power is too low notify. (APMAC=[MacAddress], APName=[STRING], ApIfIndex=[INTEGER], Ap Optical RxPower=[INTEGER](0.1uw), ApEntityPhysicalName=[OCTET], APID=[INTEGER])

The receive power of the AP's optical module is lower than the lower power threshold.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046803	Warning	equipmentAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
APMAC	Indicates the MAC address of an AP.
APName	Indicates the AP name.
ApIfIndex	Indicates the index of the AP interface on which the optical module is installed. Only the AD9430DN-24 and AD9431DN-24X support this object.
Ap Optical RxPower	Indicates the current receive power of the AP's optical module.
ApEntityPhysicalName	Indicates the name of the AP interface on which the optical module is installed. Only the AD9430DN-24 and AD9431DN-24X support this object.
APID	Indicates the AP ID.

Impact on the System

Services on the optical module are adversely affected, which probably leads to error codes, error packets, or even service interruption.

This alarm applies to Huawei certified optical modules only. For non-Huawei-certified optical modules, incorrect alarms may be generated.

Possible Causes

The receive power of the AP's optical module is lower than the lower power threshold.

Procedure

- Step 1** Check whether the type of the peer optical module matches that of the local optical module. For detailed matching rules, see **Hardware Failures > Interface Faults > An Optical Interface Cannot Turn Up** in the *Hardware Installation and Maintenance Guide* of the corresponding AP model.
- If so, go to Step 3.
 - If not, go to Step 2.
- Step 2** Replace the peer optical module with one matching the type of the local one. Then, check whether the alarm persists.
- If so, go to Step 3.
 - If not, go to Step 6.
- Step 3** Check whether the optical module is a Huawei certified optical module.
- If so, go to Step 5.
 - If not, go to Step 4.
- Step 4** Replace the optical module with a Huawei certified optical module. Then, check whether the alarm persists.
- If so, go to Step 5.
 - If not, go to Step 6.
- Step 5** Collect alarm messages, log messages, and configurations, and then contact the technical support personnel.
- Step 6** End.
- End

Related Information

[3.4.96 ALM-303046802 AP Optical Module Received Power Is Too High Notify](#)

3.4.96 ALM-303046802 AP Optical Module Received Power Is Too High Notify

Description

WLAN/4/AP_OPTICAL_RX_POWER_TOO_HIGH:OID [OID] AP optical module received power is too high notify. (APMAC=[OPAQUE], APName=[STRING],

ApIfIndex=[INTEGER], Ap Optical RxPower=[INTEGER](0.1uw),
ApEntityPhysicalName=[OCTET], APID=[INTEGER])

The receive power of the AP's optical module is higher than the upper power threshold.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046802	Warning	equipmentAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
APMAC	Indicates the MAC address of an AP.
APName	Indicates the AP name.
ApIfIndex	Indicates the index of the AP interface on which the optical module is installed. Only the AD9430DN-24 and AD9431DN-24X support this object.
Ap Optical RxPower	Indicates the current receive power of the AP's optical module.
ApEntityPhysicalName	Indicates the name of the AP interface on which the optical module is installed. Only the AD9430DN-24 and AD9431DN-24X support this object.
APID	Indicates the AP ID.

Impact on the System

Services on the optical module are adversely affected, which probably leads to error codes, error packets, or even service interruption.

This alarm applies to Huawei certified optical modules only. For non-Huawei-certified optical modules, incorrect alarms may be generated.

Possible Causes

The receive power of the AP's optical module is higher than the upper power threshold.

Procedure

- Step 1** Check whether the type of the peer optical module matches that of the local optical module. For detailed matching rules, see **Hardware Failures > Interface Faults > An Optical Interface Cannot Turn Up** in the *Hardware Installation and Maintenance Guide* of the corresponding AP model.
- If so, go to Step 3.
 - If not, go to Step 2.
- Step 2** Replace the peer optical module with one matching the type of the local one. Then, check whether the alarm persists.
- If so, go to Step 3.
 - If not, go to Step 6.
- Step 3** Check whether the optical module is a Huawei certified optical module.
- If so, go to Step 5.
 - If not, go to Step 4.
- Step 4** Replace the optical module with a Huawei certified optical module. Then, check whether the alarm persists.
- If so, go to Step 5.
 - If not, go to Step 6.
- Step 5** Collect alarm messages, log messages, and configurations, and then contact the technical support personnel.
- Step 6** End.
- End

Related Information

[3.4.95 ALM-303046803 AP Optical Module Received Power Is Too Low Notify](#)

3.4.97 ALM-303046804 AP Optical Module Temperature Is Too High Notify

Description

WLAN/4/AP_OPTICAL_TEMPERATURE_TOO_HIGH:OID [OID] AP optical module temperature is too high notify. (APMAC=[MacAddress], APName=[STRING], ApIfIndex=[INTEGER], Ap Optical Temperature=[INTEGER]°C, ApEntityPhysicalName=[OCTET], APID=[INTEGER])

The temperature of AP's optical module is higher than the upper temperature threshold.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046804	Warning	equipmentAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
APMAC	Indicates the MAC address of an AP.
APName	Indicates the AP name.
ApIfIndex	Indicates the index of the AP interface on which the optical module is installed. Only the AD9430DN-24 and AD9431DN-24X support this object.
Ap Optical Temperature	Indicates the temperature of the AP's optical module.
ApEntityPhysicalName	Indicates the name of the AP interface on which the optical module is installed. Only the AD9430DN-24 and AD9431DN-24X support this object.
APID	Indicates the AP ID.

Impact on the System

None

Possible Causes

The temperature of AP's optical module is higher than the upper temperature threshold.

Procedure

- Step 1**
Reduce service traffic on the AP.
 - If the alarm persists, go to Step 4.
 - If the alarm is cleared, go to Step 5.
- Step 2**
Collect alarm messages, log messages, and configurations, and then contact the technical support personnel.
- Step 3**
End.
- End**

Related Information

3.4.98 ALM-303046805 AP Optical Module Temperature Is Too Low Notify

3.4.98 ALM-303046805 AP Optical Module Temperature Is Too Low Notify

Description

WLAN/4/AP_OPTICAL_TEMPERATURE_TOO_LOW:OID [OID] AP optical module temperature is too low notify. (APMAC=[MacAddress], APName=[STRING], ApIfIndex=[INTEGER], Ap Optical Temperature=[INTEGER]°C, ApEntityPhysicalName=[OCTET], APID=[INTEGER])

The temperature of AP's optical module is lower than the lower temperature threshold.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046805	Warning	equipmentAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
APMAC	Indicates the MAC address of an AP.
APName	Indicates the AP name.
ApIfIndex	Indicates the index of the AP interface on which the optical module is installed. Only the AD9430DN-24 and AD9431DN-24X support this object.
Ap Optical Temperature	Indicates the temperature of the AP's optical module.
ApEntityPhysicalName	Indicates the name of the AP interface on which the optical module is installed. Only the AD9430DN-24 and AD9431DN-24X support this object.
APID	Indicates the AP ID.

Impact on the System

None

Possible Causes

The temperature of AP's optical module is lower than the lower temperature threshold.

Procedure

Step 1 Add service traffic on the AP.

- If the alarm persists, go to Step 4.
- If the alarm is cleared, go to Step 5.

Step 2 Collect alarm messages, log messages, and configurations, and then contact the technical support personnel.

Step 3 End.

----End

Related Information

[3.4.97 ALM-303046804 AP Optical Module Temperature Is Too High Notify](#)

3.4.99 ALM-303046806 The AP Does Not Support the Country Code Configured on the WAC

Description

WLAN/4/AP_UN SUPPORT_COUNTRY_CODE:OID [OID] AP not support configured country code notify.(APMAC=[MacAddress], APName=[STRING], COUNTRY CODE=[OCTET], APID=[INTEGER])

The AP does not support the country code configured on the AC.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046806	Warning	equipmentAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
APMAC	Indicates the MAC address of an AP.

Name	Meaning
APName	Indicates the AP name.
COUNTRY CODE	Indicates the country code configured on the AP.
APID	Indicates the AP ID.

Impact on the System

The AP cannot get online.

Possible Causes

A country code not supported by the AP is configured on the AC.

Procedure

- Step 1** Run the **display regulatory-domain-profile** { **all** | **name** *profile-name* } command to check whether the country code configured on the AC is the same as that supported by the AP.
- If the country codes are the same, go to Step 3.
 - If the country codes are different, go to Step 2.
- Step 2** Run the **country-code** *country-code* command to set the country code of the AC to the one supported by the AP.
- If the alarm persists, go to Step 4.
 - If the alarm is cleared, go to Step 5.
- Step 3** Collect alarm messages, log messages, and configurations, and then contact the technical support personnel.
- Step 4** End.
- End

Related Information

None

3.4.100 ALM-303046807 The AP Cold Boot

Description

WLAN/4/AP_COLD_BOOT:OID [OID] The AP cold boot. (APMAC=[MacAddress], AP TYPE=[OCTET], AP Sys Name=[OCTET], AP Sys Time=[OCTET], AP Alarm name=[OCTET], APID=[INTEGER])

The AP was cold started. After the AP was disconnected because of power-off, it connected to the AC again and operated properly.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046807	Warning	environmentalAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
APMAC	Indicates the MAC address of an AP.
AP TYPE	Indicates the AP type.
AP Sys Name	Indicates the AP name.
AP Sys Time	Indicates the time when the alarm is generated.
AP Alarm name	Indicates the alarm name.
APID	Indicates the AP ID.

Impact on the System

Services are interrupted after the AP is disconnected from the AC.

NOTE

This alarm was triggered simultaneously with the alarm WLAN_1.3.6.1.4.1.2011.6.139.13.1.1.31 hwApColdBootRestoreTrap (the AP restored after a cold restart).

Possible Causes

The AP is powered on, goes online, and operates properly after an unexpected disconnection.

Procedure

- Step 1** Check whether the power supply of the AP is working properly. Then, check whether the alarm persists.
- If so, go to Step 2.
 - If not, go to Step 3.
- Step 2** Collect alarm messages, log messages, and configurations, and then contact the technical support personnel.

Step 3 End.
----End

Related Information

None

3.4.101 ALM-303046808 AP Hot Boot

Description

WLAN/4/AP_HOT_BOOT:OID [OID] AP hot boot. (APMAC=[OPAQUE], APTYPE=[OCTET], APName=[OCTET], APOccurTime=[OCTET], NotifyName=[OCTET], APID=[INTEGER])
An AP is hot started.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046808	Warning	environmentalAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
APMAC	Indicates the MAC address of an AP.
APType	Indicates the AP type.
APName	Indicates the AP name.
APOccurTime	Indicates the time when the alarm is generated.
NotifyName	Indicates the alarm name.
APID	Indicates the AP ID.

Impact on the System

The AP cannot work and its services are interrupted after a manual restart.

Possible Causes

The AP is manually restarted.

Procedure

- Step 1** Check whether the AP had been restarted. Then, check whether the alarm persists.
- If so, go to Step 2.
 - If not, go to Step 3.
- Step 2** Collect alarm messages, log messages, and configurations, and then contact the technical support personnel.
- Step 3** End.
- End

Related Information

None

3.4.102 ALM-303046809 AP CRC Is Abnormal Notify

Description

WLAN/4/AP_CRC_TOO_HIGH:OID [OID] AP CRC is abnormal notify.
(APMAC=[OPAQUE], APName=[STRING], APCrcErrRate=[LONG]/10000,
PortType=[OCTET], PortID=[INTEGER], APID=[INTEGER])

The number of CRC error packets collected at a specified sampling interval exceeded the threshold.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046809	Warning	environmentalAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
APMAC	Indicates the MAC address of an AP.
APName	Indicates the AP name.
APCrcErrRate	Indicates the number of CRC error packets.
PortType	Indicates the AP port type.
PortID	Indicates the AP port number.
APID	Indicates the AP ID.

Impact on the System

None

Possible Causes

The number of CRC error packets collected at a specified sampling interval exceeded the threshold.

Procedure

- Step 1** Run the **display port-link-profile { all | name *profile-name* }** command to check whether the configured alarm threshold for CRC errors is proper.
- If so, go to Step 3.
 - If not, go to Step 2.
- Step 2** Run the **crc-alarm enable [high-threshold *high-threshold-value* | low-threshold *low-threshold-value*]*** command to set a proper alarm threshold for CRC errors.
- If the alarm persists, go to Step 3.
 - If the alarm is cleared, go to Step 4.
- Step 3** Collect alarm messages, log messages, and configurations, and then contact the technical support personnel.
- Step 4** End.
- End

3.4.103 ALM-303046811 Report AP Name Conflict

Description

WLAN/4/AP_NAME_CONFLICT:OID [OID] Report ap name conflict.
(APMAC=[OPAQUE], APReportName=[OCTET], APOccurTime=[OCTET],
APID=[INTEGER])

The name of a new online AP reported to the AC conflicts with that of an existing online AP.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046811	Warning	equipmentAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.

Name	Meaning
ApMac	Indicates the MAC address of an AP.
ApName	Indicates the AP name.
APOccurTime	Indicates the time when the alarm is generated.
APID	Indicates the AP ID.

Impact on the System

Two different APs use the same name, causing a failure in AP information query based on the AP name.

Possible Causes

The name configured on the AP conflicts with that of an online AP on the AC.

Procedure

- Step 1** Log in to the AP and run the **ap-rename { ap-name *name* | ap-mac *ap-mac-address* | ap-id *ap-id* } new-name *ap-new-name*** command to modify the name of the AP to prevent name conflict.
- Step 2** Restart the AP. Then, check whether the alarm persists.
- If so, go to Step 3.
 - If not, go to Step 4.
- Step 3** Collect alarm messages, log messages, and configurations, and then contact the technical support personnel.
- Step 4** End.

----End

Related Information

None

3.4.104 ALM-303046812 AP License Notify

Description

WLAN/4/AP_NUM_REACH_LICENSE_UPLIMIT:OID [OID] AP License Notify. (Info = [OCTET])

AP specific license resources were insufficient (the number of online APs reached the maximum).

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046812	Warning	equipmentAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
Info	Indicates AP license information.

Impact on the System

New APs cannot go online.

Possible Causes

The number of online APs reached the maximum value specified by the license.

Procedure

Step 1 Purchase new licenses or add new ACs to increase the maximum number of online APs. Then, check whether the alarm persists.

- If so, go to Step 2.
- If not, go to Step 3.

Step 2 Collect alarm messages, log messages, and configurations, and then contact the technical support personnel.

Step 3 End.

----End

Related Information

None

3.4.105 ALM-303046813 AP IIC Channel Fault

Description

WLAN/4/AP_FMEA_FAULT_IIC_CHANNEL:OID [OID] AP IIC channel fault. (AP MAC=[OPAQUE], APName=[STRING], APID=[INTEGER])

The AP's IIC channel fails.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046813	Warning	equipmentAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
APMAC	Indicates the MAC address of an AP.
APName	Indicates the AP name.
APID	Indicates the AP ID.

Impact on the System

The AP cannot properly work.

Possible Causes

The AP's IIC channel fails.

Procedure

- Step 1** Check whether services are affected.
- If so, go to Step 2.
 - If not, go to Step 4.
- Step 2** Restart the AP. Then, check whether the alarm persists.
- If so, go to Step 3.
 - If not, go to Step 5.
- Step 3** Replace the faulty AP. Then, check whether the alarm persists.
- If so, go to Step 4.
 - If not, go to Step 5.
- Step 4** Collect alarm messages, log messages, and configurations, and then contact the technical support personnel.
- Step 5** End.
- End

Related Information

None

3.4.106 ALM-303046814 AP PHY CMOS Fault

Description

WLAN/4/AP_FMEA_FAULT_PHY_CMOS:OID [OID] AP PHY CMOS fault.
(APMAC=[OPAQUE], APName=[STRING], APID=[INTEGER])

The AP's PHY chip fails.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046814	Warning	equipmentAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
APMAC	Indicates the MAC address of an AP.
APName	Indicates the AP name.
APID	Indicates the AP ID.

Impact on the System

The AP cannot properly work.

Possible Causes

The AP's PHY chip fails.

Procedure

- Step 1** Check whether services are affected.
- If so, go to Step 2.
 - If not, go to Step 4.
- Step 2** Restart the AP. Then, check whether the alarm persists.
- If so, go to Step 3.
 - If not, go to Step 5.
- Step 3** Replace the faulty AP. Then, check whether the alarm persists.
- If so, go to Step 4.

- If not, go to Step 5.

Step 4 Collect alarm messages, log messages, and configurations, and then contact the technical support personnel.

Step 5 End.

----End

Related Information

None

3.4.107 ALM-303046815 AP FMEA Fault

Description

WLAN/2/AP_FMEA_FAULT:OID [OID] AP FMEA fault. (APMAC=[OPAQUE], APName=[STRING], FaultID=[INTEGER], Index=[INTEGER], FaultInfo=[STRING], APID=[INTEGER])

The AP generates an alarm when a hardware fault occurs.

NOTE

If a device generates a Failure Mode Effect Analysis (FMEA) alarm, the hardware circuit, module, or chip of the device becomes faulty.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046815	Warning	equipmentAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
APMAC	Indicates the MAC address of the AP generating the hardware fault alarm.
APName	Indicates the name of the AP generating the hardware fault alarm.
FaultID	Indicates the index of the AP fault.
Index	Indicates the AP interface.
FaultInfo	Describes the AP fault.
APID	Indicates the AP ID.

Impact on the System

The AP cannot properly work.

Possible Causes

AP Fault Index	Possible Cause
1	The PHY chip is abnormal.
2	The CPLD logic is abnormal.
3	The temperature sensor is abnormal.
4	The optical module is abnormal.
5	The Wi-Fi chip or PCIE is abnormal.
6	The LSW is abnormal.
7	Wi-Fi radio initialization failed.
8	Ethernet interface initialization failed.
9	The PSE input voltage is abnormal.
10	The PSE chip is abnormal.
11	An exception occurs on the USB flash drive.
12	The bad block rate for the NAND flash exceeds the threshold.
13	The voltage failed.
14	The double-edge connector failed.
15	The reset button failed.
16	The Bluetooth function failed.
17	The CPU failed.
18	The IIC of the PCA failed.

Procedure

Step 1 Check whether the value of **FaultID** is **4**.

- If so, go to Step 2.
- If not, go to Step 6.

Step 2 Check whether the type of the peer optical module matches that of the local optical module. For detailed matching rules, see **Hardware Failures > Interface Faults > An Optical Interface Cannot Turn Up** in the *Hardware Installation and Maintenance Guide* of the corresponding AP model.

- If so, go to Step 4.
- If not, go to Step 3.

Step 3 Replace the peer optical module with one matching the type of the local one. Then, check whether the alarm persists.

- If so, go to Step 4.
- If not, go to Step 10.

Step 4 Check whether the optical module is a Huawei certified optical module.

- If so, go to Step 9.
- If not, go to Step 5.

Step 5 Replace the optical module with a Huawei certified optical module. Then, check whether the alarm persists.

- If so, go to Step 9.
- If not, go to Step 10.

Step 6 Check whether services are affected.

- If so, go to Step 7.
- If not, go to Step 9.

Step 7 Restart the AP. Then, check whether the alarm persists.

- If so, go to Step 8.
- If not, go to Step 10.

Step 8 Replace the faulty AP. Then, check whether the alarm persists.

- If so, go to Step 9.
- If not, go to Step 10.

Step 9 Collect alarm messages, log messages, and configurations, and then contact the technical support personnel.

Step 10 End.

----End

Related Information

None

3.4.108 ALM-303046922 AP Optical Insert

Description

WLAN/4/AP_OPTICAL_INSERT:OID [OID] AP optical insert. (APMAC=[OPAQUE], APName=[STRING], IfIndex=[INTEGER], ApEntityPhysicalName=[OCTET], APID=[INTEGER])

An alarm is generated when an optical module is installed on an AP.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046922	Warning	equipmentAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
APMAC	Indicates the MAC address of the AP on which an optical module is installed.
APName	Indicates the name of the AP on which an optical module is installed.
IfIndex	Indicates the index of the AP interface on which an optical module is installed.
ApEntityPhysicalName	Indicates the name of the AP interface on which the optical module is installed. Only the AD9430DN-24 and AD9431DN-24X support this object.
APID	Indicates the AP ID.

Impact on the System

None

Possible Causes

An optical module is installed on the AP.

Procedure

Step 1 This alarm is informational only, and no action is required.

----End

Related Information

[3.4.109 ALM-303046923 AP Optical Remove](#)

3.4.109 ALM-303046923 AP Optical Remove

Description

WLAN/4/AP_OPTICAL_REMOVE:OID [OID] AP optical remove.
(APMAC=[OPAQUE], APName=[STRING], IfIndex=[INTEGER],
ApEntityPhysicalName=[OCTET], APID=[INTEGER])

An alarm is generated when an optical module is removed from an AP.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046923	Warning	equipmentAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
APMAC	Indicates the MAC address of the AP from which an optical module is removed.
APName	Indicates the name of the AP on which an optical module is removed.
IfIndex	Indicates the index of the AP interface on which an optical module is installed.
ApEntityPhysicalName	Indicates the name of the AP interface on which the optical module is installed. Only the AD9430DN-24 and AD9431DN-24X support this object.
APID	Indicates the AP ID.

Impact on the System

The AP cannot provide optical module functions.

Possible Causes

An optical module is removed from the AP.

Procedure

- Step 1** This alarm is informational only, and no action is required.
 ----End

Related Information

[3.4.108 ALM-303046922 AP Optical Insert](#)

3.4.110 ALM-303046400 AP Receive Invalid ARP New Trap

Description

WLAN/4/AP_RECEIVED_INVALID_ARP_PACKET:OID [OID] AP received invalid arp packet notify.(APMAC=[OPAQUE], APName=[STRING], RadioID=[INTEGER], WlanID=[INTEGER], Drop Num=[INTEGER], APID=[INTEGER])
 The AP receives invalid ARP packets.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046400	Warning	equipmentAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
APMAC	Indicates the MAC address of an AP.
APName	Indicates the AP name.
RadioID	Indicates the ID of the radio under attack.
WlanID	Indicates the WLAN ID reporting the alarm.
Drop Num	Indicates the number of dropped packets.
APID	Indicates the AP ID.

Impact on the System

None

Possible Causes

The AP receives invalid ARP packets.

Procedure

Step 1 Check whether the AP is attacked by ARP packets from rogue devices under assistant of technical support personnel.

----End

Related Information

None

3.4.111 ALM-303046924 AP Software Version Is Not Match with AC Software Version

Description

WLAN/4/AP_SOFTWARE_VERSION_MISMATCH:OID [OID] AP software version is not match with AC software version.(APMAC=[OPAQUE], APName=[STRING], APTYPE=[OCTET], APSoftWareVersion=[OCTET], APID=[INTEGER])

The AP's version does not match the AC's.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046924	Warning	equipmentAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
APMAC	Indicates the MAC address of an AP.
APName	Indicates the AP name.
APType	Indicates the AP type.
APSoftWareVersion	Indicates the software version of the AP.
APID	Indicates the AP ID.

Impact on the System

The AP cannot provide WLAN services.

Possible Causes

The AP's version does not match the AC's.

Procedure

Step 1 Upgrade the AP to the target version according to the *AC Upgrade Guide*.

----End

Related Information

None

3.4.112 ALM-303046782 Upload Remote Capture File Notify

Description

WLAN/4/RADIO_UPLOAD_REMOTE_CAPTURE_FILE_RESULT:OID [OID] Upload remote capture file notify. (APMAC=[OPAQUE], APName=[STRING], RadioID=[INTEGER], Info = [OCTET], APID=[INTEGER])

This alarm describes upload results of remote packet capturing files.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046782	Warning	equipmentAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
APMAC	Indicates the MAC address of an AP.
APName	Indicates the AP name.
RadioID	Indicates the radio ID of the AP.
Info	Indicates upload results of remote packet capturing files.
APID	Indicates the AP ID.

Impact on the System

None

Possible Causes

The AP has uploaded remote packet capturing files.

Procedure

Step 1 This alarm is informational only, and no action is required.

----End

Related Information

None

3.4.113 ALM-303046757 MP Reached AC through the Ethernet Port Notify

Description

WLAN/4/MP_JOINED_ON_ETHERNET:OID [OID] MP reached AC through the Ethernet port,and this MP doesn't setup mesh link in avoid of loopback.
(APMAC=[OPAQUE], APName=[STRING], APID=[INTEGER])

An MP goes online through an Ethernet interface.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046757	Warning	Communication alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
APMAC	Indicates the MAC address of an AP.
APName	Indicates the AP name.
APID	Indicates the AP ID.

Impact on the System

None

Possible Causes

An MP goes online through an Ethernet interface.

Procedure

Step 1 This alarm is informational only, and no action is required.

----End

Related Information

None

3.4.114 ALM-303046758 MPP Joins AC through the Air Notify

Description

WLAN/4/MPP_JOINED_ON_AIR:OID [OID] MPP can't reach AC through the Ethernet port,so this MPP joins AC through the air,changes itself to MP,and forbid traffic on the Ethernet port in avoid of loopback. (APMAC=[OPAQUE], APName=[STRING], APID=[INTEGER])

An MPP changes to an MP and goes online through an air interface.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046758	Warning	Communication alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
APMAC	Indicates the MAC address of an AP.
APName	Indicates the AP name.
APID	Indicates the AP ID.

Impact on the System

None

Possible Causes

Due to a link fault, an MPP changes to an MP and goes online through an air interface.

Procedure

Step 1 This alarm is informational only, and no action is required.

----End

Related Information

None

3.4.115 ALM-303046927 AP Optical Module Transfer Power Is Too High Notify

Description

WLAN/4/AP_OPTICAL_TX_POWER_TOO_HIGH:OID [OID] AP optical module transfer power is too high notify. (APMAC=[OPAQUE], APName=[STRING], ApIfIndex=[INTEGER], Ap Optical TxPower=[INTEGER](0.1uw), ApEntityPhysicalName=[OCTET], APID=[INTEGER])

The transmit power of the AP's optical module exceeded the upper threshold.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046927	Warning	equipmentAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
APMAC	Indicates the MAC address of an AP.
APName	Indicates the AP name.
ApIfIndex	Indicates the index of the AP interface on which the optical module is installed. Only the AD9430DN-24 and AD9431DN-24X support this object.

Name	Meaning
Ap Optical TxPower	Indicates the current transmit power of the AP's optical module.
ApEntityPhysicalName	Indicates the name of the AP interface on which the optical module is installed. Only the AD9430DN-24 and AD9431DN-24X support this object.
APID	Indicates the AP ID.

Impact on the System

Services on the optical module are adversely affected, which probably leads to error codes, error packets, or even service interruption.

This alarm applies to Huawei certified optical modules only. For non-Huawei-certified optical modules, incorrect alarms may be generated.

Possible Causes

The transmit power of the AP's optical module exceeded the upper threshold.

Procedure

- Step 1** Check whether the type of the peer optical module matches that of the local optical module. For detailed matching rules, see **Hardware Failures > Interface Faults > An Optical Interface Cannot Turn Up** in the *Hardware Installation and Maintenance Guide* of the corresponding AP model.
- If so, go to Step 3.
 - If not, go to Step 2.
- Step 2** Replace the peer optical module with one matching the type of the local one. Then, check whether the alarm persists.
- If so, go to Step 3.
 - If not, go to Step 6.
- Step 3** Check whether the optical module is a Huawei certified optical module.
- If so, go to Step 5.
 - If not, go to Step 4.
- Step 4** Replace the optical module with a Huawei certified optical module. Then, check whether the alarm persists.
- If so, go to Step 5.
 - If not, go to Step 6.
- Step 5** Collect alarm messages, log messages, and configurations, and then contact the technical support personnel.

Step 6 End.
----End

Related Information

[3.4.116 ALM-303046938 AP Optical Module Transfer Power Is Too Low Notify](#)

3.4.116 ALM-303046938 AP Optical Module Transfer Power Is Too Low Notify

Description

WLAN/4/AP_OPTICAL_TX_POWER_TOO_LOW:OID [OID] AP optical module transfer power is too low notify. (APMAC=[MacAddress], APName=[STRING], ApIfIndex=[INTEGER], Ap Optical TxPower=[INTEGER](0.1uw), ApEntityPhysicalName=[OCTET], APID=[INTEGER])
The transmit power of the AP's optical module fell below the lower threshold.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046938	Warning	equipmentAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
APMAC	Indicates the MAC address of an AP.
APName	Indicates the AP name.
ApIfIndex	Indicates the index of the AP interface on which the optical module is installed. Only the AD9430DN-24 and AD9431DN-24X support this object.
Ap Optical TxPower	Indicates the current transmit power of the AP's optical module.
ApEntityPhysicalName	Indicates the name of the AP interface on which the optical module is installed. Only the AD9430DN-24 and AD9431DN-24X support this object.

Name	Meaning
APID	Indicates the AP ID.

Impact on the System

Services on the optical module are adversely affected, which probably leads to error codes, error packets, or even service interruption.

This alarm applies to Huawei certified optical modules only. For non-Huawei-certified optical modules, incorrect alarms may be generated.

Possible Causes

The transmit power of the AP's optical module fell below the lower threshold.

Procedure

- Step 1** Check whether the type of the peer optical module matches that of the local optical module. For detailed matching rules, see **Hardware Failures > Interface Faults > An Optical Interface Cannot Turn Up** in the *Hardware Installation and Maintenance Guide* of the corresponding AP model.
- If so, go to Step 3.
 - If not, go to Step 2.
- Step 2** Replace the peer optical module with one matching the type of the local one. Then, check whether the alarm persists.
- If so, go to Step 3.
 - If not, go to Step 6.
- Step 3** Check whether the optical module is a Huawei certified optical module.
- If so, go to Step 5.
 - If not, go to Step 4.
- Step 4** Replace the optical module with a Huawei certified optical module. Then, check whether the alarm persists.
- If so, go to Step 5.
 - If not, go to Step 6.
- Step 5** Collect alarm messages, log messages, and configurations, and then contact the technical support personnel.
- Step 6** End.
- End

Related Information

[3.4.115 ALM-303046927 AP Optical Module Transfer Power Is Too High Notify](#)

3.4.117 ALM-303046939 All Functions of the Fan Module Failed

Description

WLAN/4/AP_FAN_INVALID:OID [OID] All functions of the fan module failed.
(APMAC=[OPAQUE], APName=[STRING], ApFanIndex=[INTEGER],
ApEntityPhysicalName=[OCTET], APID=[INTEGER])

The alarm is generated when fans become faulty.

Only the AD9430DN-24 and AD9431DN-24X support this object.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046939	Warning	equipmentAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
APMAC	Indicates the AP's MAC address.
APName	Indicates the AP name.
ApFanIndex	Indicates the interface index of the AP fan.
ApEntityPhysicalName	Indicates the AP interface name.
APID	Indicates the AP ID.

Impact on the System

The temperature of boards becomes high.

Possible Causes

Fans are faulty.

Procedure

- Step 1** Run the **display fan** command on AD9430DN-24 or AD9431DN-24X to check the fan status. Check whether the fan tray is registered and the fan speed is zero.
- If the fan tray is not registered, remove and install the fan tray.

- If the fan speed is zero, replace the fan.
- If the fault persists, contact technical support personnel.
- End

Related Information

None

3.4.118 ALM-303046940 A Storage Card Is Removed.

Description

WLAN/4/AP_STORAGE_CARD_REMOVE:OID [OID] A storage card is removed. (APMAC=[OPAQUE], APName=[STRING], ApStorageIndex=[INTEGER], ApStorageName=[OCTET], APID=[INTEGER])

This alarm is generated when a storage card is removed.

Only the AD9430DN-24 and AD9431DN-24X support this object.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046940	Warning	equipmentAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
APMAC	Indicates the AP's MAC address.
APName	Indicates the AP name.
ApStorageIndex	Indicates the interface index of the storage card.
ApStorageName	Indicates the name of the storage card.
APID	Indicates the AP ID.

Impact on the System

If the alarm is displayed when the storage device is in position, the configuration file and log file may be lost.

Possible Causes

The storage device is pulled out.

Procedure

- Check whether the storage device is removed. If not, contact the technical support personnel.

Related Information

None

3.4.119 ALM-303046401 A Storage Card Is Inserted

Description

WLAN/4/AP_STORAGE_CARD_INSERT:OID [OID] A storage card is inserted.
(APMAC=[OPAQUE], APName=[STRING], ApStorageIndex=[INTEGER],
ApStorageName=[OCTET], APID=[INTEGER])

This alarm is generated when a storage card is inserted.

Only the AD9430DN-24 and AD9431DN-24X support this object.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046401	Warning	equipmentAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
APMAC	Indicates the AP's MAC address.
APName	Indicates the AP name.
ApStorageIndex	Indicates the interface index of the storage card.
ApStorageName	Indicates the name of the storage card.
APID	Indicates the AP ID.

Impact on the System

None

Possible Causes

A storage device is inserted.

Procedure

- Check whether the storage device is inserted. If not, contact the technical support personnel.

Related Information

None

3.4.120 ALM-303046941 A Port Is Powered off.

Description

WLAN/4/AP_POE_POWER_OFF:OID [OID] A port is powered off.
(APMAC=[OPAQUE], APName=[STRING], ApIfIndex=[INTEGER],
ApEntityPhysicalName=[OCTET], APID=[INTEGER], Reason=[STRING])

The PD connected to the interface is powered off.

Only the AP4050DN-E, AP4050DN-HD, AP7050DN-E, AP7052DN, AP7152DN, AD9430DN-24, AD9431DN-24X and AD9430DN-12 support this alarm.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046941	Warning	equipmentAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
APMAC	Indicates the AP's MAC address.
APName	Indicates the AP name.
ApIfIndex	Indicates the AP interface index.
ApEntityPhysicalName	Indicates the AP interface name.
APID	Indicates the AP ID.

Name	Meaning
Reason	Indicates the power-off reason.

Impact on the System

The PD connected to the interface is powered off and cannot work normally.

Possible Causes

Cause 1: The PD is removed.

Cause 2: The PD is faulty.

Cause 3: When the power is insufficient, the interface with higher priority preempts the power.

Cause 4: The interface is automatically powered off in the power-off time range.

Procedure

Step 1 Check whether the PD is removed.

- If so, go to step 2.
- If not, go to step 3.

Step 2 Install the PD and check whether the alarm is cleared.

- If so, go to step 11.
- If not, go to step 3.

Step 3 Check whether the power is sufficient.

- If so, go to step 7.
- If not, go to step 4.

Step 4 Check whether the priority of the interface is low.

- If so, go to step 5.
- If not, go to step 8.

Step 5 Check whether the interface priority is proper according to the requirements for the interface priority.

- If yes, use the **poe priority (AP wired port link profile view)** command to re-set the interface priority.
- If not, increase the PoE power.

Step 6 Check whether the alarm is cleared.

- If so, go to step 11.
- If not, go to step 7.

Step 7 Check whether the PD is faulty.

- If so, go to step 8.

- If not, go to step 9.

Step 8 Replace the PD and check whether the alarm is cleared.

- If so, go to step 11.
- If not, go to step 9.

Step 9 Check whether the interface is in the power-off time range.

- If so, go to step 11.
- If not, go to step 10.

Step 10 Contact technical support personnel.

Step 11 End

----End

Related Information

[3.4.121 ALM-303046402 A Port Is Powered on.](#)

3.4.121 ALM-303046402 A Port Is Powered on.

Description

WLAN/4/AP_POE_POWER_ON:OID [OID] A port is powered on.
(APMAC=[OPAQUE], APName=[STRING], ApIfIndex=[INTEGER],
ApEntityPhysicalName=[OCTET], APID=[INTEGER])

The interface meets the following power supply conditions:

- The power is sufficient.
- The PD is identified by the system.

Only the AP4050DN-E, AP4050DN-HD, AP7050DN-E, AP7052DN, AP7152DN,
AD9430DN-24, AD9431DN-24X and AD9430DN-12 support this alarm.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046402	Warning	equipmentAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
APMAC	Indicates the AP's MAC address.
APName	Indicates the AP name.

Name	Meaning
ApIfIndex	Indicates the AP interface index.
ApEntityPhysicalName	Indicates the AP interface name.
APID	Indicates the AP ID.

Impact on the System

Services are not affected.

Possible Causes

The alarm recovery message is generated after power-off.

Procedure

- This alarm indicates that a fault is rectified, and no action is required.

Related Information

[3.4.120 ALM-303046941 A Port Is Powered off.](#)

3.4.122 ALM-303046942 A Port Detects Connection of A PD

Description

WLAN/4/AP_POE_PD_CONNECTED:OID [OID] A port detects connection of a PD.
(APMAC=[OPAQUE], APName=[STRING], ApIfIndex=[INTEGER],
ApEntityPhysicalName=[OCTET], APID=[INTEGER])

The PD is connected to an interface.

Only the AP4050DN-E, AP4050DN-HD, AP7050DN-E, AP7052DN, AP7152DN,
AD9430DN-24, AD9431DN-24X and AD9430DN-12 support this alarm.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046942	Warning	equipmentAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.

Name	Meaning
APMAC	Indicates the AP's MAC address.
APName	Indicates the AP name.
ApIfIndex	Indicates the AP interface index.
ApEntityPhysicalName	Indicates the AP interface name.
APID	Indicates the AP ID.

Impact on the System

Services are not affected.

Possible Causes

The system detects a valid PD.

Procedure

Step 1 A new PD is added. This alarm is informational and no action is required.

----End

Related Information

None

3.4.123 ALM-303046407 A Port Detects Disconnection of A PD

Description

WLAN/4/AP_POE_PD_DISCONNECTED:OID [OID] A port detects disconnection of a PD. (APMAC=[OPAQUE], APName=[STRING], ApIfIndex=[INTEGER], ApEntityPhysicalName=[OCTET], APID=[INTEGER])

The PD is disconnected from an interface.

Only the AP4050DN-E, AP4050DN-HD, AP7050DN-E, AP7052DN, AP7152DN, AD9430DN-24, AD9431DN-24X and AD9430DN-12 support this alarm.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046407	Warning	equipmentAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
APMAC	Indicates the AP's MAC address.
APName	Indicates the AP name.
ApIfIndex	Indicates the AP interface index.
ApEntityPhysicalName	Indicates the AP interface.
APID	Indicates the AP ID.

Impact on the System

The PD is unavailable and services are not affected.

Possible Causes

A valid PD is removed.

Procedure

Step 1 Check whether the PD is removed.

- If yes, go to step 3.
- If not, go to step 2.

Step 2 Reinstall the PD.

Step 3 End.

----End

Related Information

None

3.4.124 ALM-303046943 A Port Detects A PD Whose Current Exceeds the Threshold of the Corresponding Class.

Description

WLAN/4/AP_POE_PD_CLASS_OVER_CURRENT:OID [OID] A port detects a PD whose current exceeds the threshold of the corresponding class.
(APMAC=[OPAQUE], APName=[STRING], ApIfIndex=[INTEGER],
ApEntityPhysicalName=[OCTET], APID=[INTEGER])

The system detects that overcurrent occurs during PD classification and does not provide power for PDs.

Only the AP4050DN-E, AP4050DN-HD, AP7050DN-E, AP7052DN, AP7152DN, AD9430DN-24, AD9431DN-24X and AD9430DN-12 support this alarm.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046943	Warning	Communication alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
APMAC	Indicates the AP's MAC address.
APName	Indicates the AP name.
ApIfIndex	Indicates the AP interface index.
ApEntityPhysicalName	Indicates the AP interface name.
APID	Indicates the AP ID.

Impact on the System

Services are not affected.

Possible Causes

The PD does not comply with standards.

Procedure

Step 1 You can run the **poe high-inrush enable (AP system profile view)** command in the AP system profile view to configure an interface to allow generation of the high pulse current. Then check whether the alarm is cleared.

- If yes, go to step 4.
- If not, go to step 2.

Step 2 Replace the PD and check whether the alarm is cleared.

- If yes, go to step 4.
- If not, go to step 3.

Step 3 Contact technical support personnel.

Step 4 End.

----End

Related Information

None

3.4.125 ALM-303046954 The Port Priority Is Different from the PD Priority

Description

WLAN/4/AP_POE_PD_PRIORITY_DIFFERENT:OID [OID] The port priority is different from the PD priority. (APMAC=[OPAQUE], APName=[STRING], ApIfIndex=[INTEGER], ApEntityPhysicalName=[OCTET], ApPoePdPriority=[INTEGER], ApPoePortPriority=[INTEGER], APID=[INTEGER])

The interface priority is different from the PD priority.

Only the AP4050DN-E, AP4050DN-HD, AP7050DN-E, AP7052DN, AP7152DN, AD9430DN-24, AD9431DN-24X and AD9430DN-12 support this alarm.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046954	Warning	Quality of service alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
APMAC	Indicates the AP's MAC address.
APName	Indicates the AP name.
ApIfIndex	Indicates the AP interface index.
ApEntityPhysicalName	Indicates the AP interface name.
ApPoePdPriority	Indicates the PD priority.
ApPoePortPriority	Indicates the interface priority.
APID	Indicates the AP ID.

Impact on the System

Services are not affected.

Possible Causes

The interface priority is low, whereas the PD priority is high.

Procedure

Step 1 Run the **poe priority (AP wired port link profile view)** command to change the interface priority to be higher than the PD priority. Then, check whether the alarm persists.

- If so, go to Step 2.
- If not, go to Step 3.

Step 2 Collect alarm messages, log messages, and configurations, and then contact the technical support personnel.

Step 3 End.

----End

Related Information

None

3.4.126 ALM-303046955 The Power Load of A PoE Card Exceeds the Upper Limit.

Description

WLAN/4/AP_POE_POWER_OVER_UTILIZATION_THRESHOLD:OID [OID] The power load of a PoE card exceeds the upper limit. (APMAC=[OPAQUE], APName=[STRING], ApIfIndex=[INTEGER], ApEntityPhysicalName=[OCTET], ApPoeCurConsumPower=[INTEGER], ApPoeConsumPowerThreshold=[INTEGER], APID=[INTEGER])

The total PoE power consumption is greater than or equal to the alarm threshold.

Only the AP4050DN-E, AP4050DN-HD, AP7050DN-E, AP7052DN, AP7152DN, AD9430DN-24, AD9431DN-24X and AD9430DN-12 support this alarm.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046955	Warning	equipmentAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.

Name	Meaning
APMAC	Indicates the AP's MAC address.
APName	Indicates the AP name.
ApIfIndex	Indicates the AP interface index.
ApEntityPhysicalName	Indicates the AP interface name.
ApPoeCurConsumPower	Indicates the current consumed power.
ApPoeConsumPowerThreshold	Indicates the power threshold.
APID	Indicates the AP ID.

Impact on the System

If the alarm persists, all the PDs may be powered off because of insufficient power supply.

Possible Causes

The total power consumption of all the PDs is greater than or equal to the alarm threshold.

Procedure

- Step 1
- Plan the network according to the system power supply. Increase priorities of important devices to prevent their power from being preempted. If the alarm persists, power off some PDs to ensure system reliability.

----End

Related Information

None

3.4.127 ALM-303046956 Interface Has Turned into DOWN State

Description

WLAN/4/AP_STP_AUTO_SHUTDOWN:OID [OID] Interface has turned into DOWN state. (APMAC=[OPAQUE], APName=[STRING], ApIfIndex=[INTEGER], ApEntityPhysicalName=[OCTET], APID=[INTEGER])

An alarm is generated when STP detects a local loopback and triggers port shutdown.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046956	Warning	equipmentAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object of the alarm.
APMAC	Indicates the MAC address of the AP.
APName	Indicates the AP name.
ApIfIndex	Indicates the AP interface index.
ApEntityPhysicalName	Indicates the AP interface name.
APID	Indicates the AP ID.

Impact on the System

When STP detects a local loopback, it determines that a network storm occurs and will trigger shutdown of the local interface to prevent the storm from affecting services on the entire network; however, services on the shutdown interface will be interrupted.

Possible Causes

After STP detects a loopback on an interface, the device shuts down the interface to prevent a loop.

Procedure

- Step 1** Check whether local loopback is configured on the interface where the alarm is generated.
 - Y=>4
 - N=>2
- Step 2** Check whether a hub is incorrectly connected on the network connected to the interface.
 - Y=>5
 - N=>3
- Step 3** Collect alarm information, log information, and configuration information, and then contact technical support personnel.
- Step 4** Delete configurations that cause the local loopback.

Step 5 Remove the self-looped cable.

Step 6 End

----End

Related Information

None

3.4.128 ALM-303046957 The Optical Transceiver Does Not Work Normally

Description

WLAN/4/AP_OPTICAL_INVALID:OID [OID] The optical transceiver does not work normally. (APMAC=[OPAQUE], APName=[STRING], ApIfIndex=[INTEGER], ApEntityPhysicalName=[OCTET], hwWlanApOpticalFaultID=[INTEGER], APID=[INTEGER], hwWlanApOpticalFaultReason=[OCTET])

The AP's optical module is faulty.

Only the AD9430DN-24 and AD9431DN-24X support this object.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046957	Warning	equipmentAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
APMAC	Indicates the AP's MAC address.
APName	Indicates the AP name.
ApIfIndex	Indicates the AP interface index.
ApEntityPhysicalName	Indicates the AP interface name.
hwWlanApOpticalFaultID	Indicates the fault ID of the AP's optical module.
APID	Indicates the AP ID.
hwWlanApOpticalFaultReason	Indicates the reason for the fault of the AP's optical module.

Impact on the System

Services will be interrupted.

Possible Causes

The rate of the optical module does not match the interface rate.

Procedure

Step 1 Check the interface rate and replace the optical module with a proper one.

----End

Related Information

None

3.4.129 ALM-303046765 VAP Has the Max Number of Stations Notify

Description

WLAN/4/VAP_REACH_MAX_USERS:OID [OID] VAP has the max number of stations notify.(APMAC=[OPAQUE], APName=[STRING], RADIOID=[INTEGER], WLANID=[INTEGER], FailCause=[INTEGER], PermitNum=[INTEGER], APID=[INTEGER])

No station (STA) can be associated with the VAP.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046765	Warning	equipmentAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
APMAC	Indicates the MAC address of an AP.
APName	Indicates the AP name.
RADIOID	Indicates the radio ID of the AP.
WLANID	Indicates the WLAN ID reporting the alarm.

Name	Meaning
FailCause	Indicates the cause for the STA authentication failure.
PermitNum	Indicates the maximum number of STAs that can be associated with the AP.
APID	Indicates the AP ID.

Impact on the System

New STAs cannot connect to the VAP.

Possible Causes

The number of STAs connected to the VAP has reached the upper limit. New STAs cannot connect to the VAP.

Procedure

- Step 1** Check whether the maximum number of STAs allowed to connect to the SSID is proper. It is recommended that you set the maximum number of STAs to 256.
- If so, go to Step 3.
 - If not, go to Step 2.
- Step 2** In the SSID profile, run the **max-sta-number** *max-sta-number* command to change the maximum number of STAs allowed to connect to the SSID to a proper value. Check whether the alarm persists.
- If so, go to Step 3.
 - If not, go to Step 5.
- Step 3** The VAP cannot provide WLAN services to STAs. Associate new STAs to another VAP. Then, check whether the alarm persists.
- If so, go to Step 4.
 - If not, go to Step 5.
- Step 4** Collect alarm messages, log messages, and configurations, and then contact the technical support personnel.
- Step 5** End.
- End

Related Information

None

3.4.130 ALM-4287373447 the Number of Users Connected to the AP Exceeds the Alarm Threshold

Description

WLAN/4/VAP_REACH_MAX_USERS_RESTORE:OID [OID] VAP has the max number of stations notify restore.(APMAC=[OPAQUE], APName=[STRING], RADIOID=[INTEGER], WLANID=[INTEGER], FailCause=[INTEGER], CurrentNum=[INTEGER], APID=[INTEGER])

The alarm about a VAP's failure to connect STAs is cleared.

Attribute

Alarm ID	Alarm Severity	Alarm Type
4287373447	Minor	equipmentAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
APMAC	Indicates the MAC address of an AP.
APName	Indicates the AP name.
RADIOID	Indicates the radio ID of the AP.
WLANID	Indicates the WLAN ID reporting the alarm.
FailCause	Indicates the cause for the STA authentication failure.
CurrentNum	Indicates the current number of STAs that can be associated with the AP.
APID	Indicates the AP ID.

Impact on the System

New STAs can connect to the VAP.

Possible Causes

The number of STAs is smaller than the maximum number.

Procedure

Step 1 This alarm is informational only, and no action is required.

----End

Related Information

None

3.4.131 ALM-3416068 Low Power of A BLE Device

Description

WLAN/4/BLE_LOW_POWER: OID [OID] The battery is low at the BLE site.
(BLEMAC=[OPAQUE])

The battery power of a BLE device is lower than the specified low power alarm threshold for BLE devices.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3416068	Warning	equipmentAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object of the alarm.
BLEMAC	Indicates the MAC address of a BLE device.

Impact on the System

If the battery is exhausted, a BLE device cannot work properly.

Possible Causes

The battery power of the BLE device is lower than the specified low power alarm threshold for BLE devices.

Procedure

Step 1 Replace the battery of the BLE device.

----End

Related Information

None

3.4.132 ALM-3416069 A BLE Device Goes Offline

Description

WLAN/4/BLE_OFFLINE: OID [OID] An exception occurs at the BLE site.
(BLEMAC=[OPAQUE])

A BLE device gets offline.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3416069	Warning	equipmentAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object of the alarm.
BLEMAC	Indicates the MAC address of a BLE device.

Impact on the System

A BLE device cannot work normally after getting offline.

Possible Causes

The system cannot detect the signal from the BLE device for over 30 minutes.

Procedure

- Step 1** Check the operating status of the BLE device.
- If the BLE device works abnormally, go to step 2.
 - If the BLE device works normally, go to step 3.
- Step 2** Ensure that the BLE device can work normally.
- If the alarm persists, go to step 3.
 - If the alarm is cleared, go to step 4.
- Step 3** Collect information about alarms, logs, and configurations, and then contact technical support personnel.

Step 4 This alarm is informational only, and no action is required.

----End

Related Information

None

3.4.133 ALM-3416070 Built-in Bluetooth Module Fault

Description

WLAN/4/INNER_BLE_BROKEN: OID [OID] The AP's internal BLE module fails.
(APMAC=[OPAQUE], APName=[STRING], APID=[INTEGER])

An AP's built-in Bluetooth module is faulty.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3416070	Warning	equipmentAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object of the alarm.
APMAC	Indicates the MAC address of an AP.
APName	Indicates the name of an AP.
APID	Indicates the ID of an AP.

Impact on the System

The AP's built-in Bluetooth module cannot work normally.

Possible Causes

The system did not detect heartbeat messages from the AP's built-in Bluetooth module for 32 seconds.

Procedure

Step 1 Check the operating status of the AP's built-in Bluetooth module.

- If the AP's built-in Bluetooth module works abnormally, go to step 2.
- If the AP's built-in Bluetooth module works normally, go to step 3.

- Step 2** Ensure that the AP's built-in Bluetooth module can work properly.
- If the alarm persists, go to step 3.
 - If the alarm is cleared, go to step 4.
- Step 3** Collect information about alarms, logs, and configurations, and then contact technical support personnel.
- Step 4** This alarm is informational only, and no action is required.
- End

Related Information

None

3.4.134 ALM-303046972 An IoT Card Is Inserted

Description

WLAN/4/AP_IOT_CARD_INSERT:OID [OID] A iot card is inserted.
(APMAC=[OPAQUE], APName=[STRING], AplotCardId=[INTEGER],
APID=[INTEGER])

An IoT card is inserted.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046972	Warning	processingErrorAlarm

Parameters

Name	Meaning
OID	ID of a MIB object.
APMAC	MAC address of an AP.
APName	Name of an AP.
AplotCardId	Number of the slot on an AP where an IoT card is installed.
APID	ID of an AP.

Impact on the System

If a card from Enjoyor is inserted, the AP restarts. Inserting a card from Prime Electronics & Satellitics Inc. has no impact on the system.

Possible Causes

An IoT card is inserted.

Procedure

Step 1 This alarm is informational only, and no action is required.

----End

Related Information

[3.4.135 ALM-303046406 An IoT Card Is Removed](#)

3.4.135 ALM-303046406 An IoT Card Is Removed

Description

WLAN/4/AP_IOT_CARD_REMOVE:OID [OID] A iot card is removed.
(APMAC=[OPAQUE], APName=[STRING], AplotCardId=[INTEGER],
APID=[INTEGER])

An IoT card is removed.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046406	Warning	processingErrorAlarm

Parameters

Name	Meaning
OID	ID of a MIB object.
APMAC	MAC address of an AP.
APName	Name of an AP.
AplotCardId	Number of the slot on an AP where an IoT card is installed.
APID	ID of an AP.

Impact on the System

If a card from Enjoyor is removed, the AP restarts. Removing a card from Prime Electronics & Satellitics Inc. has no impact on the system.

Possible Causes

An IoT card is removed.

Procedure

Step 1 This alarm is informational only, and no action is required.

----End

Related Information

[3.4.134 ALM-303046972 An IoT Card Is Inserted](#)

3.4.136 ALM-303046973 Failed to Start the Server Used By the IoT Card

Description

WLAN/2/AP_IOT_SERVER_START_FAIL:OID [OID] Failed to start the server used by the IoT card. (Cause: The UDP port is occupied.) (APMAC=[OPAQUE], APName=[STRING], AplotCardId=[INTEGER], UdpPort=[INTEGER], APID=[INTEGER])

The server module on an AP for receiving data from the IoT card fails to start.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046973	Major	Communication alarm

Parameters

Name	Meaning
OID	ID of a MIB object.
APMAC	MAC address of an AP.
APName	Name of an AP.
AplotCardId	Number of the slot on an AP where an IoT card is installed.
UdpPort	UDP port number.
APID	ID of an AP.

Impact on the System

The server module on an AP for receiving data from the IoT card fails to start, and services are not available.

Possible Causes

The port used by the server module on the AP for receiving data from the IoT card is occupied.

Procedure

Step 1 Change the IP address and port number.

----End

Related Information

None

3.4.137 ALM-303046974 SubFirmware Is Not Match AP Version

Description

WLAN/4/AP_SUBFIRMWARE_MISMATCH:OID [OID] SubFirmware is not match AP version. (APMAC=[OPAQUE], APName=[STRING], APSubFirmwareName=[STRING], APSubFirmware=[INTEGER], RealVersion=[STRING], ExpectVersion=[STRING], APID=[INTEGER])

The sub-firmware version on the AP mismatches.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046974	Warning	processingErrorAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object of the alarm.
APMAC	Indicates the AP's MAC address.
APName	Indicates the AP's name.
APSubFirmwareName	Indicates the AP's sub-firmware name.
APSubFirmware	Indicates the AP's sub-firmware number.

Name	Meaning
RealVersion	Indicates the actual version of the AP's sub-firmware.
APID	Indicates the AP ID.

Impact on the System

Version mismatch may cause faulty communication of the sub-firmware and affect functions of the sub-firmware.

Possible Causes

The sub-firmware upgrade fails and rolls back.

Procedure

- Step 1 Restart the AP and upgrade the sub-firmware again.
- Step 2 If the fault persists, contact technical support personnel.
- End

Related Information

None

3.4.138 ALM-303046783 the AP Configuration Is Inconsistent with the Actual Attribute

Description

WLAN/4/AP_CONFIG_INCONSIST_WITH_ACTUAL:OID [OID] The AP configuration is inconsistent with the actual attribute. (APMAC=[OPAQUE], APName=[STRING], APID=[INTEGER], Config=[OCTET], Reason=[OCTET])

The configuration of an AP is inconsistent with the actual attribute.

 NOTE

This alarm is supported only by the AP4051TN, AP8130DN, AP8130DN-W, and AP4030TN.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046783	Warning	equipmentAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object of the alarm.
APMAC	Indicates the AP's MAC address.
APName	Indicates the AP name.
APID	Indicates the AP ID.
Config	Indicates the configuration.
Reason	Indicates the reason for the configuration inconsistency.

Impact on the System

None

Possible Causes

The actual radio frequency band of an AP is different from that configured on the AC.

Procedure

- Step 1

Change the AP's radio frequency band to the actual one. Check whether the alarm persists.

If so, go to Step 2.

If not, go to Step 3.
- Step 2

Collect trap, log, and configuration information, and contact Huawei technical support personnel.
- Step 3

End.
- End

Related Information

None

3.4.139 ALM-303046987 the BLE Site Detached

Description

WLAN/4/BLE_DETACHED:OID [OID] The BLE site detached.
(BLEMAC=[OPAQUE(hex)])

An AP detected that a Bluetooth tag was detached.

 NOTE

Only the AP2050DN-E, AP2051DN-E, AP4050DN-E, AP4051TN, AP6052DN, AP7050DE, AP7052DE, AP7052DN, AP4050DE-M, AP4050DE-M-S, AP4050DE-B-S, AP7060DN, AP6750-10T, AP7152DN, AP8050DN, AP8050DN-S, AP8050TN-HD, AP8082DN, AP8150DN, AP8182DN, R250D-E, and R251D-E support this alarm.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046987	Warning	equipmentAlarm

Parameters

Name	Meaning
OID	Indicates the ID of the alarm MIB object.
BLEMAC	Indicates the MAC address of a Bluetooth tag.

Impact on the System

After a Bluetooth tag is detached from an asset, the asset cannot be accurately located using Bluetooth location signals.

Possible Causes

The Bluetooth tag was detached from the asset.

Procedure

- Step 1** Check the Bluetooth tag location on the location server based on the Bluetooth tag location result. Find the Bluetooth tag and re-attach it to the asset.

----End

Related Information

None

3.4.140 ALM-303046991 AP Power Supply Is Insufficient

Description

WLAN/2/POWER_INSUFF:OID [OID] AP power supply is insufficient.
(APMAC=[OPAQUE], APName=[STRING], PowerWorkMode=[OCTET],
ExpectPowerWorkMode=[OCTET], APID=[INTEGER],impact=[OCTET])

The AP power supply was insufficient.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046991	Major	equipmentAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object of the alarm.
APMAC	Indicates the AP MAC address.
APName	Indicates the AP name.
PowerWorkMode	Indicates the actual power supply mode of the AP.
ExpectPowerWorkMode	Indicates the expected power supply mode of the AP.
APID	Indicates the AP ID.
Impact	Impact of Insufficient Power Supply on AP.

Impact on the System

The AP restarts due to insufficient power supply.

Possible Causes

The power supply is insufficient for the AP.

Procedure

- Step 1** Run the **lldp enable** command in the interface view to enable the LLDP function. In this way, the peer power supply device can identify the power supply standard of the local device and supply power as required.
- If the alarm persists, go to step 2.
 - If the alarm is cleared, go to step 4.
- Step 2** Check the peer power supply device and ensure that the power supply standard meets the AP's power supply requirements.
- If the alarm persists, go to step 3.
 - If the alarm is cleared, go to step 4.

Step 3 Collect alarm and configuration information, and contact technical support personnel.

Step 4 End.

----End

Related Information

None

3.4.141 ALM-303046982 Interface Receive Insecure Mac-address

Description

WLAN/4/INSECURE_MAC:OID [OID] Interface receive insecure mac-address.
(APMAC=[OPAQUE], APName=[STRING], IllegalMAC=[OPAQUE],
VLANID=[INTEGER], InterfaceName=[OCTET], APID=[INTEGER])

An interface on an AP received a packet with an unauthorized MAC address.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046982	Warning	environmentalAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object of the alarm.
APMAC	Indicates the MAC address of the AP.
APName	Indicates the AP name.
IllegalMAC	Indicates the unauthorized MAC address.
VLANID	Indicates the VLAN ID.
InterfaceName	Indicates the interface name.
APID	Indicates the AP ID.

Impact on the System

None

Possible Causes

When the number of secure MAC addresses learned by the interface reached the maximum, the interface received a packet with an unauthorized MAC address.

Procedure

Step 1 Check whether an unauthorized device is connected to the AP's interface.

----End

Related Information

None

3.4.142 ALM-303046983 the Number of Multicast and Broadcast Packets Received on the AP Exceeds the Threshold 1000 pps for 10 Seconds

Description

WLAN/4/MCBC_EXCEED:OID [OID] The number of multicast and broadcast packets received on the AP exceeds the threshold 1000 pps for 10 seconds. (APMAC=[OPAQUE], APName=[STRING], APID=[INTEGER])

The number of multicast and broadcast packets reported by an AP exceeded the alarm threshold.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046983	Warning	Alarm

Parameters

Name	Meaning
OID	Indicates the ID of the alarm MIB object.
APMAC	Indicates the MAC address of an AP.
APName	Indicates the AP name.
APID	Indicates the AP ID.

Impact on the System

If an AP reported too many multicast and broadcast packets, AP services are affected.

Possible Causes

The number of multicast and broadcast packets reported by the AP exceeded the alarm threshold.

Procedure

- Step 1** Check the networking, find senders of the multicast and broadcast packets, and optimize the networking. Check whether the alarm persists.
- If so, go to Step 2.
 - If not, go to Step 4.
- Step 2** Run the **traffic-optimize broadcast-suppression enable** command in the AP system profile view to enable the rate limit for broadcast packets and IGMP multicast packets on the AP. Check whether the alarm persists.
- If so, go to Step 3.
 - If not, go to Step 4.
- Step 3** Collect alarm, log, and configuration information, and contact technical support personnel.
- Step 4** End.
- End

3.4.143 ALM-303046984 the Configured and Reported AP Types Are Different

Description

WLAN/4/AP_TYPE_MISMATCH:OID [OID] The configured and reported AP types are different.(APMAC=[OPAQUE], APName=[STRING], APConfigType=[STRING], APActualType=[STRING], APID=[INTEGER])

The AP type configured on the AC did not match the actual AP type.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046984	Warning	equipmentAlarm

Parameters

Name	Meaning
OID	Indicates the ID of the alarm MIB object.
APMAC	Indicates the AP's MAC address.
APName	Indicates the AP name.
APConfigType	Indicates the configured AP type.
APActualType	Indicates the actual AP type.
APID	Indicates the AP ID.

Impact on the System

The AP fails to go online.

Possible Causes

The AP type configured on the AC did not match the actual AP type.

Procedure

Step 1 Configure the correct AP type.

----End

3.4.144 ALM-303046985 An AP Detects that the Soft-GRE Tunnel Is Down

Description

WLAN/4/AP_DETECT_SOFTGRE_DOWN:OID [OID] AP detect softgre tunnel down notify.(APMAC=[OPAQUE], DstIP=[IPADDR], APName=[STRING], APID=[INTEGER])

An AP detects that the Soft-GRE tunnel is Down.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046985	Major	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the ID of the alarm MIB object.
APMAC	Indicates the MAC address of an AP.
DstIP	Indicates the destination IP address.
APName	Indicates the AP name.
APID	Indicates the AP ID.

Impact on the System

User traffic cannot be forwarded through the Soft-GRE tunnel.

Possible Causes

- After keepalive is enabled, the AP fails to ping the ME60.
- The Soft-GRE configuration is incorrect on the ME60. The ME60 does not respond to keepalive messages from the AP.
- The link between the AP and ME60 is torn down.

Procedure

- Step 1** Check whether the Soft-GRE function is enabled on the VE interface of the Soft-GRE tunnel.
 - Step 2** Check whether the IP address is correctly configured on the loopback interface.
 - Step 3** Check whether the Soft-GRE group is bound to the VE interface and loopback interface.
 - Step 4** Check whether the ME60 can ping the AP.
 - Step 5** Collect trap, log, and configuration information, and contact technical support personnel.
- End

3.4.145 ALM-303046992 the AP Version Is Not Recommended for the Current AC

Description

- WLAN/4/AP_VERSION_NOT_RECOMMENDED_TRAP:OID [OID] The AP version is not recommended for the current AC.
- The AP version is not recommended for the current AC.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046992	Warning	Quality of service alarm

Parameters

Name	Meaning
OID	Indicates the MIB object of the alarm.

Impact on the System

The load balancing effect may be affected.

Possible Causes

The AP version is not recommended for the current AC.

Procedure

Upgrade involved APs to the recommended version.

3.4.146 ALM-303046404 the Disk Usage of An AP Exceeds the Upper Threshold

Description

WLAN/4/AP_DISK_OVERLOAD:OID [OID] The Disk usage of an AP exceeds the upper threshold.(APMAC=[OPAQUE], APName=[STRING],APDiskThresholdWarning=[INTEGER],APDiskThresholdCurrent=[INTEGER],APID=[INTEGER])

The disk usage exceeds the upper alarm threshold.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046404	Warning	equipmentAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object of the alarm.
APMAC	Indicates the AP's MAC address.
APName	Indicates the AP name.
APDiskThresholdWarning	Indicates the disk usage alarm threshold of the AP.
APDiskThresholdCurrent	Indicates the current hard disk usage of the AP.
APID	Indicates the AP ID.

Impact on the System

The configuration may fail to be saved.

Possible Causes

This object indicates that the AP's disk space is fully occupied.

Procedure

Step 1 Run the **dir** command in the user view to check files in the system.

Step 2 Run the **delete [/unreserved]** command to delete unnecessary files.

Files that can be deleted include those that are saved by the user and generated using commands, as well as the following in the system inventory:

- **logfile**: stores log files, which can be exported and then deleted.
- **corefile**: stores exception information files, which can be exported and then deleted.

Step 3 Collect alarms, logs, and configurations, and then contact technical support personnel.

Step 4 End.

----End

3.4.147 ALM-303046405 the AP Works in Limited Mode Due to Insufficient Power Supply

Description

WLAN/4/AP_POWER_LIMITED: OID[OID] The AP works in Limited mode due to insufficient power supply.(APMAC=[OPAQUE], APName=[STRING], PowerWorkMode=[OCTET], ExpectPowerWorkMode=[OCTET], APID=[INTEGER])

The AP power supply is insufficient, and the AP works in Limited mode.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046405	Warning	equipmentAlarm

Parameters

Name	Meaning
OID	Indicates the ID of a MIB object.
APMAC	Indicates the AP MAC address.
APName	Indicates the AP name.
PowerWorkMode	Indicates the actual power supply mode of the AP.
ExpectPowerWorkMode	Indicates the expected power supply mode of the AP.
APID	Indicates the AP ID.

Impact on the System

When an AP works with low power consumption, some component functions such as the USB and PoE out functions are disabled. In addition, radio power is reduced, or radios are disabled. For details, see the functions of APs using different power supply standards in **Device Management Configuration Guide > PoE Configuration > Understanding PoE** in the *FATAP, Cloud APV200R019C10 Configuration Guide*.

Possible Causes

The device that supplies power to the AP does not meet the AP's power supply requirements.

Procedure

- Step 1** Run the **lldp enable** command in the interface view to enable the LLDP function. In this way, the peer power supply device can identify the power supply standard of the local device and supply power as required.
- If the alarm persists, go to step 2.
 - If the alarm is cleared, go to step 4.
- Step 2** Check the peer power supply device and ensure that the power supply standard meets the AP's power supply requirements.

- If the alarm persists, go to step 3.
- If the alarm is cleared, go to step 4.

Step 3 Collect alarm and configuration information, and contact technical support personnel.

Step 4 End.

----End

Related Information

None

3.4.148 ALM-303046738 the AP Works in Limited Mode Due to Insufficient Power Supply

Description

ENTITYTRAP/4/AP_POWER_LIMITED:OID [OID] The AP works in Limited mode due to insufficient power supply.(APWorkMode=[OCTET], ExpectWorkMode=[OCTET])

The AP power supply is insufficient, and the AP works in Limited mode.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046738	Warning	equipmentAlarm

Parameters

Name	Meaning
OID	Indicates the ID of a MIB object.
APWorkMode	Indicates the actual power supply mode of an AP.
ExpectWorkMode	Indicates the expected power supply mode of an AP.

Impact on the System

When an AP works with low power consumption, some component functions such as the USB and PoE out functions are disabled. In addition, radio power is reduced, or radios are disabled. For details, see the functions of APs using different power supply standards in **Device Management Configuration GuidePoE ConfigurationUnderstanding PoE** in the *FATAP, Cloud APV200R019C10 Configuration Guide*.

Possible Causes

The device that supplies power to the AP does not meet the AP's power supply requirements.

Procedure

- Step 1** Run the **lldp enable** command in the interface view to enable the LLDP function. In this way, the peer power supply device can identify the power supply standard of the local device and supply power as required.
- If the alarm persists, go to step 2.
 - If the alarm is cleared, go to step 4.
- Step 2** Check the peer power supply device and ensure that the power supply standard meets the AP's power supply requirements.
- If the alarm persists, go to step 3.
 - If the alarm is cleared, go to step 4.
- Step 3** Collect alarm and configuration information, and contact technical support personnel.
- Step 4** End.

----End

Related Information

None

3.4.149 ALM-303046794 AP Begins to Update

Description

WLAN/4/AP_UPDATE_BEGIN:OID [OID] AP begins to update. Do not power off the AP during the upgrade. (APMAC=[OPAQUE], APName=[STRING], APID=[INTEGER])

The AP began to upgrade.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046794	Warning	equipmentAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.

Name	Meaning
APMAC	Indicates the MAC address of an AP.
APName	Indicates the AP name.
APID	Indicates the AP ID.

Impact on the System

None

Possible Causes

The AP was upgraded.

Procedure

Step 1 This alarm is informational only, and no action is required.

----End

Related Information

None

3.4.150 ALM-303046408 AP Upgrade Finished

Description

WLAN/4/AP_UPDATE_RESULT:OID [OID] AP updates completely.
(APMAC=[OPAQUE],
APName=[STRING],UpdateResult=[INTEGER],UpdateTime=[OCTET],UpdateFileName=[OCTET],UpdateNextOper=[INTEGER], UpdateStatus=[STRING],
APID=[INTEGER])

AP upgrade finished.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046408	Warning	equipmentAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
APMAC	Indicates the MAC address of an AP.
APName	Indicates the AP name.
UpdateResult	Indicates the AP upgrade result.
UpdateTime	Indicates the AP upgrade time.
UpdateFileName	Indicates the AP upgrade file name.
UpdateNextOper	Indicates the operation after upgrade.
UpdateStatus	Indicates the AP upgrade result status.
APID	Indicates the AP ID.

Impact on the System

Services will not be affected after the successful upgrade.

APs and AP-based services cannot work properly after the failed automatic upgrade.

APs cannot be updated to the new version after the failed online upgrade. However, current services are not affected.

Possible Causes

AP upgrade finished or failed.

Procedure

- Step 1** Check the upgrade result according to alarm parameters.
- If AP upgrade succeeded, go to Step 10.
 - If AP upgrade failed, go to Step 2.
- Step 2** Run the **display ap update configuration** command to view the AP upgrade mode.
- If the FTP mode is used, go to Step 3.
 - If the AC mode is used, go to Step 6.
- Step 3** Run the **display ap update configuration** command to check whether the FTP upgrade mode is correctly configured.
- If not, run the **ap update ftp-server** command to modify the configuration. And then go to Step 8.
 - If so, go to Step 4.

- Step 4** Check whether an upgrade file exists on the FTP server.
- If not, store the correct files on the FTP server. And then go to Step 8.
 - If so, go to Step 5.
- Step 5** Check whether the network connection between the AP and FTP server works properly.
- If not, rectify the network fault, and try again. And then go to Step 8.
 - If so, go to Step 7.
- Step 6** Run the **dir** command to check whether there is an upgrade file in the flash memory on the AC.
- If not, load correct files to the AC. And then go to Step 8.
 - If so, go to Step 7.
- Step 7** Check whether upgrade files are correct.
- If not, reload or store these files, and try again. And then go to Step 8.
 - If so, go to Step 9.
- Step 8** Check whether the upgrade succeeds.
- If so, go to Step 10.
 - If not, go to Step 9.
- Step 9** Collect the alarm information, log information, and configuration information, and then contact technical support personnel.
- Step 10** End.
- End

Related Information

None

3.4.151 ALM-303046810 The U-boot Version Does Not Match the AP Version

Description

WLAN/4/AP_UBOOT_MISMATCH:OID [OID] AP uboot is not match AP version.
(APMAC=[OPAQUE], APName=[STRING], APID=[INTEGER])

The U-boot version does not match the AP version.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046810	Warning	processingErrorAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
APMac	Indicates the MAC address of an AP.
APName	Indicates the AP name.
APID	Indicates the AP ID.

Impact on the System

The AP cannot work properly because of upgrade failures.

Possible Causes

The U-boot version does not match the AP version.

Procedure

- Step 1** Contact the technical support personnel to obtain the AP version matches the U-boot version.
- Step 2** Upgrade the AP according to the *AC Upgrade Guide*. Then, check whether the alarm persists.
- If so, go to Step 3.
 - If not, go to Step 4.
- Step 3** Collect alarm messages, log messages, and configurations, and then contact the technical support personnel.
- Step 4** End.
- End

Related Information

None

3.4.152 ALM-303046790 Detected Rogue Device

Description

WLAN/4/WIDS_DETECT_DEVICE:OID [OID] Detected rogue device. (Device Mac=[OPAQUE], Device type=[INTEGER], Device channel=[INTEGER], Device RSSI=[LONG], Device ssid=[OCTET], Monitor APName=[OCTET], Monitor APMAC=[OPAQUE], Monitor AP radio =[INTEGER], Monitor AP ID=[INTEGER]).

This alarm is generated when an unauthorized device is detected.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046790	Warning	environmentalAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
Device Mac	Indicates the MAC address of an unauthorized device.
Device type	Indicates the type of an unauthorized device. • 1: AP • 2: Adhoc • 3: Bridge • 4: STA
Device channel	Indicates the channel of an unauthorized device.
Device RSSI	Indicates the RSSI of an unauthorized device.
Device ssid	Indicates the SSID of an unauthorized device.
Monitor APName	Indicates the name of a monitoring AP.
Monitor APMAC	Indicates the MAC address of a monitoring AP.
Monitor AP radio	Indicates the radio ID of a monitoring AP.
Monitor AP ID	Indicates the ID of a monitoring AP.

Impact on the System

None

Possible Causes

An unauthorized device was detected.

Procedure

- Step 1** Take countermeasures against the detected unauthorized device and configure WIPS.
1. Enter the AP group radio view or the AP radio view and run the **wids contain enable** command to enable rogue device containment.
 2. Enter the WIDS profile view and run the **contain-mode** command to configure the countermeasures mode of the AP.
- Step 2** Then, check whether the alarm persists.
- If so, go to Step 2.
 - If not, go to Step 3.
- Step 3** Collect alarm messages, log messages, and configurations, and then contact the technical support personnel.
- Step 4** End.

----End

Related Information

None

3.4.153 ALM-303046784 Detected Rogue Devices

Description

WLAN/4/WIDS_DETECT_ROGUE_DEVICE:OID [OID] Detected rogue devices.
(Device count=[INTEGER])

The alarm is generated when rogue devices are detected.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046784	Warning	environmentalAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
Device count	Indicates the number of rogue devices.

Impact on the System

Rogue devices exist in the current air interface environment and may affect air interface performance.

Possible Causes

Rogue devices are detected.

Procedure

- Step 1** Check the number of rogue devices and impact on services.
- If only a few rogue devices exist and services are not affected, no action is required.
 - If services are affected, go to Step 2.
- Step 2** Run the **display wlan ids device-detected all** command to check all detected rogue devices.
- Step 3** Contain detected rogue devices and configure WIDS rogue device containment.
1. Enter the AP group radio view or AP radio view, and run the **wids contain enable** command to enable rogue device containment.
 2. Enter the WIDS profile view and run the **contain-mode** command to configure the rogue device containment mode for APs.
- Step 4** Check whether the alarm persists.
- If so, go to Step 6.
 - If not, go to Step 7.
- Step 5** Collect alarm, log, and configuration information, and contact technical support personnel.
- Step 6** End.
- End

Related Information

None

3.4.154 ALM-303046785 Detected Attack Devices

Description

WLAN/4/WIDS_DETECT_ATTACK:OID [OID] Detected attack devices. (Device count=[INTEGER])

This alarm is generated when attack devices are detected.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046785	Warning	environmentalAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
Device count	Indicates the number of attack devices.

Impact on the System

Attack devices exist in the current air interface environment and may affect air interface performance.

Possible Causes

Attack devices are detected.

Procedure

- Step 1** Check the number of attack devices and impact on services.
- If only a few attack devices exist and services are not affected, no action is required.
 - If services are affected, go to Step 2.
- Step 2** Run the **display wlan ids attack-detected all** command to check all detected attack devices.
- Step 3** Run the **dynamic-blacklist enable** command in the WIDS profile view to enable the dynamic blacklist function.
- Step 4** Check whether the alarm persists.
- If so, go to Step 5.
 - If not, go to Step 6.
- Step 5** Collect alarm, log, and configuration information, and contact technical support personnel.
- Step 6** End.
- End

Related Information

None

3.4.155 ALM-303046786 Detected non-Wi-Fi Devices

Description

WLAN/4/WIDS_DETECT_NON_WIFI:OID [OID] Detected non-Wi-Fi devices. (Device count=[INTEGER])

This alarm is generated when non-Wi-Fi devices are detected.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046786	Warning	environmentalAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
Device count	Indicates the number of non-Wi-Fi devices.

Impact on the System

Non-Wi-Fi devices exist in the current air interface environment and may affect air interface performance.

Possible Causes

Non-Wi-Fi devices are detected.

Procedure

- Step 1** Check the number of non-Wi-Fi devices and impact on services.
 - If only a few non-Wi-Fi devices exist and services are not affected, no action is required.
 - If services are affected, go to Step 2.
- Step 2** Run the **display wlan non-wifi-device all** command to check all detected non-Wi-Fi devices.
- Step 3** Set the radio calibration policy to **non-wifi** or change the AP's working channel to avoid interference of non-Wi-Fi devices.
- Step 4** Check whether the alarm persists.
 - If so, go to Step 5.

- If not, go to Step 6.

Step 5 Collect alarm, log, and configuration information, and contact technical support personnel.

Step 6 End.

----End

Related Information

None

3.4.156 ALM-303046773 Channel of Radio Is Changed

Description

WLAN/4/RADIO_CHANNEL_CHANGE:OID [OID] Channel of radio is changed.
(APMAC=[OPAQUE], RadioID=[INTEGER], APName=[OCTET], Channel1=[OCTET], Channel2=[OCTET], CauseId=[INTEGER], CauseStr=[OCTET], PreChannel1=[OCTET], PreChannel2=[OCTET], APID=[INTEGER], NewChannelHasRadarChannel=[OCTET])

The AP channel was changed.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046773	Warning	environmentalAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
APMAC	Indicates the MAC address of an AP.
RadioID	Indicates the radio ID.
APName	Indicates the AP name.
Channel1	Indicates the actual working channel of the AP.
Channel2	Indicates the actual second working channel of the AP.

Name	Meaning
CauseId	Indicates the channel change reason. • unknown(1) - The channel was changed due to an unknown reason. • dfs(2) - The channel was changed due to Dynamic Frequency Selection (DFS). • wds(3) - The channel was changed due to WDS network establishment. • config(4) - The channel was changed due to manual configurations. • calibrate(5) - The channel was changed due to radio calibration. • thirdGPP(6) - The channel was changed due to 3GPP base station notification.
CauseStr	Indicates a character string describing channel change reasons.
PreChannel1	Indicates the channel before change. NOTE When an AP goes online on an AC for the first time, the channel of the AP before change is not saved on the AC. Therefore, when a channel change alarm is generated for the first time, the original channel of the AP is displayed as - in the alarm.
PreChannel2	Indicates the second channel before the channel is changed.
APID	Indicates the AP ID.
NewChannelHasRadarChannel	Indicates whether radar channels exist among the changed channels.

Impact on the System

The working channel of the AP was changed, which may affect the other APs.

Possible Causes

Cause 1: The radio was calibrated.

Cause 2: Users changed the channel.

Cause 3: Radar signals conflicted.

Cause 4: The channel changed in WDS mode.

Cause 5: The channel changed in Mesh mode.

Procedure

- Step 1
This alarm is informational only, and no action is required.
- End

Related Information

None

3.4.157 ALM-303046772 Radio Signal Environment Deteriorates

Description

WLAN/4/RADIO_ENV_DETERIORATE:OID [oid] Radio signal environment deteriorates. (APMAC=[OPAQUE], RadioID=[INTEGER], APName=[OCTET], PER=[INTEGER]%, RetransmissionRate=[INTEGER]%, APID=[INTEGER], NoiseFloor=[INTEGER]dBm, Reason=[OCTET], BadChannel=[INTEGER], InterferenceRate=[INTEGER]).

Radio signal environment deteriorates.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046772	Warning	equipmentAlarm

Parameters

Name	Meaning
OID	Indicates the ID of the MIB object.
APMAC	Indicates the MAC address of an AP.
RadioID	Indicates the radio ID.
APName	Indicates the AP name.
PER	Indicates the packet error rate on the wireless-side interface.
RetransmissionRate	Indicates the retransmission rate of a radio.
APID	Indicates the AP ID.
NoiseFloor	Indicates the noise floor value detected in the current environment.

Name	Meaning
Reason	Indicates the reason of the alarm. • ConflictRate: High retransmission rate In this case, you only need to pay attention to the parameter RetransmissionRate. Other parameters with the value 0 can be ignored. • Noise: High noise floor In this case, you only need to pay attention to the parameter NoiseFloor. Other parameters with the value 0 can be ignored. • BadChannel: Channel deterioration In this case, you only need to pay attention to the parameter BadChannel. Other parameters with the value 0 can be ignored. • InterferenceRate: High interference rate In this case, you only need to pay attention to the parameter InterferenceRate. Other parameters with the value 0 can be ignored.
BadChannel	Indicates the bad channel.
InterferenceRate	Indicates the interference rate.

Impact on the System

The frequency band of a radio is changed.

Possible Causes

The radio signal environment deteriorated.

Procedure

Step 1 Run the **display ap neighbor** command to view the neighboring radio, and check whether there are APs using the same or neighboring radio.

- If so, run the **channel** command to reconfigure a channel or power for this radio to avoid the signal interference. Then go to [Step 2](#).
- If not, go to [Step 3](#).

Step 2 Check whether a radio signal environment restoration alarm is generated.

- If so, go to [Step 6](#).
- If not, go to [Step 3](#).

Step 3 Check whether there are devices that interfere with the radio signal or make noises.

- If so, remove these devices and then go to [Step 4](#).
- If not, go to [Step 5](#).

Step 4 Check whether a radio signal environment restoration alarm is generated.

- If so, go to [Step 6](#).
- If not, go to [Step 5](#).

Step 5 Collect the alarm information, log information, and configuration information, and then contact technical support personnel.

Step 6 End.

----End

Related Information

None

3.4.158 ALM-303046774 AP work mode is changed notify

Description

WLAN/4/AP_WORK_MODE_CHANGE: OID [OID] AP work mode is changed notify.
(APMAC=[OPAQUE], RadioID=[INTEGER], APName=[OCTET], Mode=[INTEGER],
PreMode=[INTEGER], APID=[INTEGER])

The wireless monitoring mode of an AP was changed.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046774	Warning	equipmentAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
APMAC	Indicates the MAC address of an AP.
APName	Indicates the AP name.
RadioID	Indicates the radio ID.

Name	Meaning
Mode	Indicates the current wireless monitoring mode of an AP. • 0: initial status after the AP goes online • 1: normal mode • 2: monitor mode • 3: hybrid mode
PreMode	Indicates the previous wireless monitoring mode of an AP. • 0: initial status after the AP goes online • 1: normal mode • 2: monitor mode • 3: hybrid mode • 4: invalid value
APID	Indicates the AP ID.
ModeDesc	Indicates the description of the current work mode of an AP.
PreModeDesc	Indicates the description of the previous work mode of an AP.

Impact on the System

None

Possible Causes

The working mode of a radio on an AP was changed.

Procedure

Step 1 This alarm is informational only, and no action is required.

----End

Related Information

None

3.4.159 ALM-303046775 Co-Channel Interference Between APs Was Detected

Description

WLAN/4/AP_COCHANNEL_INTERFERENCE: OID [OID] The co-channel interference exceeds the alarm threshold.(APMAC=[OPAQUE], RadioID=[INTEGER], APName=[OCTET], APChannel=[INTEGER], APID=[INTEGER], IntfBssid=[OPAQUE], RSSI threshold percent=[INTEGER]%)

Co-channel interference between APs was detected.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046775	Warning	equipmentAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
APMAC	Indicates the MAC address of an AP.
APName	Indicates the AP name.
RadioID	Indicates the radio ID.
APChannel	Indicates the channel of a monitoring AP.
APID	Indicates the AP ID.
Bssid	Indicates the BSSID of the interfering AP.
RSSI threshold percent	Indicates the RSSI threshold value on an interface, in percentage.

Impact on the System

The packet loss rate increases, the data rate decreases, and even the services may be interrupted.

Possible Causes

The alarm threshold for co-channel interference was exceeded.

Procedure

- Step 1** Run the **display radio-2g-profile { all | name *profile-name* }** and **display radio-5g-profile { all | name *profile-name* }** commands to view the value of **Co-channel frequency interference threshold(%)** and check whether the alarm threshold for co-channel interference is configured properly. It is recommended that you set the alarm threshold for co-channel interference to 50.
- If so, go to Step 3.
 - If not, go to Step 2.
- Step 2** Run the **interference co-channel threshold *threshold-value*** command to configure a proper alarm threshold for co-channel interference. Then, check whether the alarm persists.
- If the alarm persists, go to Step 3.
 - If the alarm is cleared, go to Step 5.
- Step 3** If severe interference triggers local radio calibration, the channel and power are adjusted automatically. Then, check whether the alarm persists.
- If the alarm persists, go to Step 4.
 - If the alarm is cleared, go to Step 5.
- Step 4** Collect alarm messages, log messages, and configurations, and then contact the technical support personnel.
- Step 5** End.
- End

Related Information

None

3.4.160 ALM-303046776 Adjacent Channel Interference Between APs Was Detected

Description

WLAN/4/AP_ADJACENT_CHANNEL_INTERFERENCE: OID [OID] The adjacent-channel interference exceeds the alarm threshold.(APMAC=[OPAQUE], RadioID=[INTEGER],APName=[OCTET], APChannel=[INTEGER], APID=[INTEGER], IntfBssId=[OPAQUE], IntfChnl=[INTEGER], RSSI threshold percent=[INTEGER]%)

Adjacent-channel interference between APs was detected.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046776	Warning	equipmentAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
APMAC	Indicates the MAC address of an AP.
RadioID	Indicates the radio ID.
APName	Indicates the AP name.
APChannel	Indicates the channel of a monitoring AP.
APID	Indicates the AP ID.
IntfBssId	Indicates the BSSID of the interfering AP.
IntfChnl	Indicates the channel of the interfering AP.
RSSI threshold percent	Indicates the RSSI threshold value on an interface, in percentage.

Impact on the System

The packet loss rate increases, the data rate decreases, and even the services may be interrupted.

Possible Causes

The alarm threshold for adjacent-channel interference was exceeded.

Procedure

- Step 1** Run the **display radio-2g-profile { all | name *profile-name* }** and **display radio-5g-profile { all | name *profile-name* }** commands to view the value of **Adjacent-channel frequency interference threshold(%)** and check whether the alarm threshold for adjacent-channel interference is configured properly. It is recommended that you set the alarm threshold for adjacent-channel interference to 50.
- If so, go to Step 3.
 - If not, go to Step 2.
- Step 2** Run the **interference adjacent-channel threshold *threshold-value*** command to configure a proper alarm threshold for adjacent-channel interference. Then, check whether the alarm persists.
- If so, go to Step 3.
 - If not, go to Step 5.

- Step 3** If severe interference triggers local radio calibration, the channel and power are adjusted automatically. Then, check whether the alarm persists.
- If so, go to Step 4.
 - If not, go to Step 5.
- Step 4** Collect alarm messages, log messages, and configurations, and then contact the technical support personnel.
- Step 5** End.
- End

Related Information

None

3.4.161 ALM-303046777 Jam of station is detected notify

Description

WLAN/4/STA_INTERFERENCE: OID [OID] Jam of station is detected notify.
(APMAC=[OPAQUE], RadioID=[INTEGER], APName=[OCTET], APID=[INTEGER])

STA interference was detected.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046777	Warning	equipmentAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
APMAC	Indicates the MAC address of an AP.
RadioID	Indicates the radio ID.
APName	Indicates the AP name.
APID	Indicates the AP ID.

Impact on the System

If the number of interfering STAs exceeds the alarm threshold, the AP service performance is degraded.

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
APMAC	Indicates the MAC address of an AP.
RadioID	Indicates the radio ID.
APName	Indicates the AP name.
APID	Indicates the AP ID.

Impact on the System

The packet loss rate increases, the data rate decreases, and even the services may be interrupted.

Possible Causes

Devices, except for the co-channel APs, adjacent-channel APs, and STAs, worked on the AP channel and interfered with the AP.

Procedure

- Step 1**
If severe interference deteriorates the environment, it will trigger local radio calibration, and the APs will automatically adjust the channel and power. Then, check whether the alarm persists.
 - If so, go to Step 2.
 - If not, go to Step 3.
- Step 2**
Collect alarm messages, log messages, and configurations, and then contact the technical support personnel.
- Step 3**
End.

End

Related Information

None

3.4.163 ALM-303046779 AP radio is down notify

Description

WLAN/4/AP_RADIO_DOWN: OID [OID] AP radio is down notify.
(APMAC=[OPAQUE], RadioID=[INTEGER], APName=[OCTET], CauseId=[INTEGER], CauseStr=[OCTET], APID=[INTEGER])

A radio was down.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046779	Warning	equipmentAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object of the alarm.
APMAC	Indicates the MAC address of an AP.
RadioID	Indicates the radio ID.
APName	Indicates the AP name.
CauseId	Indicates the index of the radio disconnection cause.
CauseStr	Indicates the cause for a radio failure. - Radio disabled due to command execution: A radio shutdown command is delivered. - Radio disabled due to an error: An error occurs. - Radio disabled due to calibration: Radio calibration is performed. - Radio disabled due to low power consumption: The power consumption is low. - Radio disabled due to 3GPP base station notification: The 3GPP base station sends a radio shutdown instruction.
APID	Indicates the AP ID.

Impact on the System

The services on the STA are interrupted.

Possible Causes

- The radio was shut down as configured.
- The radio was shut down by radio calibration.
- Due to insufficient AP power, the AP works in low-power state.
- The radio was shut down due to a system error.

Procedure

- Step 1** No action is required when **CauseStr** is **Radio disabled due to command execution**.
- Step 2** No action is required when **CauseStr** is **Radio disabled due to calibration**.
- Step 3** No action is required when **CauseStr** is **The 3GPP base station sends a radio shutdown instruction**.
- Step 4** Check whether the power of the PoE switch connected to the AP is sufficient when **CauseStr** is **Radio disabled due to low power consumption**.
- Step 5** Collect the alarm information, log information, and configuration information, and then contact technical support personnel when **CauseStr** is **Radio disabled due to an error** or **Unexpected reason**.
- Step 6** End.
- End

Related Information

None

3.4.164 ALM-303046787 AP not support configured channel

Description

WLAN/4/AP_UN SUPPORT_CHANNEL:OID [OID] AP not support configured channel notify.(APMAC=[MacAddress],RadioID=[INTEGER], APName=[OCTET], CONFIGURED BANDWIDTH=[INTEGER], CONFIGURED CHANNEL1=[INTEGER], CONFIGURED CHANNEL2=[INTEGER], ACTUAL BANDWIDTH=[INTEGER], ACTUAL CHANNEL1=[INTEGER], ACTUAL CHANNEL2=[INTEGER], REASON=[OCTET], APID=[INTEGER])

The alarm was generated if the AP does not support the channel delivered by the AC.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046787	Warning	processingErrorAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
APMAC	Indicates the MAC address of an AP.
RadioID	Indicates the radio ID of the AP.
APName	Indicates the AP name.
CONFIGURED BANDWIDTH	Indicates the configured bandwidth.
CONFIGURED CHANNEL1	Indicates the configured channel.
CONFIGURED CHANNEL2	Indicates the configured second channel.
ACTUAL BANDWIDTH	Indicates the actual bandwidth.
ACTUAL CHANNEL1	Indicates the actual channel used.
ACTUAL CHANNEL2	Indicates the actual second channel used.
REASON	Indicates the alarm reason.
APID	Indicates the AP ID.

Impact on the System

The AP still works on the original channel. The configuration delivered from the AC does not take effect.

Possible Causes

The AP does not support the channel delivered by the AC.

Procedure

- Step 1** Check whether the AP goes online on a WDS network.
- If so, the AP does not support channel delivered. Go to Step 4.
 - If not, go to Step 2.

- Step 2** Check the channel supported by the AP and run the **channel { 20mhz | 40mhz-minus | 40mhz-plus | 80mhz | 160mhz } channel** or **channel 80+80mhz channel1 channel2** command to change the channel configured for the AP. Check whether the alarm persists.
- If so, go to Step 3.
 - If not, go to Step 4.
- Step 3** Collect alarm messages, log messages, and configurations, and then contact the technical support personnel.
- Step 4** End.
- End

Related Information

None

3.4.165 ALM-303046788 The EIRP is unlawful due to high antenna gain

Description

WLAN/4/AP_UNLAWFUL_EIRP:OID [OID] The EIRP is unlawful due to high antenna gain.(APMAC=[OPAQUE], RadioID=[INTEGER], APName=[OCTET], ConfigAntennaGain=[INTEGER], LegitimateAntennaGain=[INTEGER], APID=[INTEGER], LegitimateEIRP=[INTEGER])

The AP power is unlawful due to high antenna gain.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046788	Warning	processingErrorAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
APMAC	Indicates the MAC address of an AP.
RadioID	Indicates the radio ID of the AP.
APName	Indicates the AP name.
ConfigAntennaGain	Indicates the configured antenna gain.

Name	Meaning
LegitimateAntennaGain	Indicates the maximum legitimate antenna gain of the current AP in the current state.
APID	Indicates the AP ID.
LegitimateEIRP	Indicates the legitimate channel power.

Impact on the System

None

Possible Causes

The current antenna gain is invalid.

Procedure

- Step 1 Collect alarm messages, log messages, and configurations, and then contact the technical support personnel.
- Step 2 End.
- End

Related Information

None

3.4.166 ALM-303046789 Power of radio is changed

Description

WLAN/4/RADIO_POWER_CHANGE:OID [OID] Power of radio is changed.
(APMAC=[OPAQUE], RadioID=[INTEGER], APName=[OCTET], ACTUAL
POWER=[INTEGER], APID=[INTEGER])

The alarm is generated when the AP radio power was changed.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046789	Warning	processingErrorAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
APMAC	Indicates the MAC address of an AP.
RadioID	Indicates the radio ID of the AP.
APName	Indicates the AP name.
ACTUAL POWER	Indicates the actual power.
APID	Indicates the AP ID.

Impact on the System

None

Possible Causes

- Cause 1: A notification about the power configuration modification was sent to the AP.
- Cause 2: The global calibration was enabled.
- Cause 3: The local calibration was enabled.
- Cause 4: The periodic calibration was enabled.

Procedure

- Step 1 This alarm is informational only, and no action is required.
- End

Related Information

None

3.4.167 ALM-4287373449 The number of users associated with the AP exceeds the alarm threshold.

Description

WLAN/4/STA_NUM_EXCEED_THRESHOLD:OID [OID] AP access user number exceed threshold notify. (APMAC=[OPAQUE], RadioID=[INTEGER], APName=[OCTET], UserNum=[INTEGER], APID=[INTEGER])

The AP generates the alarm when the number of users associated with the AP exceeds the alarm threshold.

Attribute

Alarm ID	Alarm Severity	Alarm Type
4287373449	Minor	equipmentAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
ApMac	Indicates the MAC address of an AP.
APName	Indicates the AP name.
RadioID	Indicates the radio ID of the AP.
UserNum	Indicates the number of UAC users.
APID	Indicates the AP ID.

Impact on the System

When the number of users on a radio reaches the CAC threshold, the AP reports an alarm and denies access from new users. Since the system has other radios to provide services, user services will not be affected unless the number of users has exceeded the system capacity.

Possible Causes

The number of users associated with the AP radio has reached the upper limit and new users are associating with the AP radio.

Procedure

Step 1 Run the **uac client-number threshold threshold access *access-threshold* [*roam roam-threshold*]** command in the RRM profile view to increase the upper limit on the number of users. Then, check whether the alarm persists.

- If so, go to Step 2.
- If not, go to Step 3.

Step 2 Collect alarm messages, log messages, and configurations, and then contact the technical support personnel.

Step 3 End.

----End

Related Information

3.4.168 ALM-303046770 AP access user number exceed threshold notify

3.4.168 ALM-303046770 AP access user number exceed threshold notify

Description

WLAN/4/STA_NUM_EXCEED_THRESHOLD_RESTORE:OID [OID] AP access user number exceed threshold notify restore. (APMAC=[OPAQUE], RadioID=[INTEGER], APName=[OCTET], UserNum=[INTEGER], APID=[INTEGER])

The AP generates the alarm clearance notification when the number of users associated with the AP falls below the alarm threshold.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046770	Warning	equipmentAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
ApMac	Indicates the MAC address of an AP.
APName	Indicates the AP name.
RadioID	Indicates the radio ID of the AP.
UserNum	Indicates the number of UAC users.
APID	Indicates the AP ID.

Impact on the System

None

Possible Causes

The number of users associated with the AP falls below the alarm threshold.

Procedure

Step 1 This alarm is informational only, and no action is required.

----End

Related Information

[3.4.167 ALM-4287373449 The number of users associated with the AP exceeds the alarm threshold.](#)

3.4.169 ALM-4287373448 The number of roaming users connected to the AP exceeds the alarm threshold

Description

WLAN/4/ROAM_STA_NUM_EXCEED_THRESHOLD:OID [OID] AP roam user number exceed threshold notify. (APMAC=[OPAQUE], RadioID=[INTEGER], APName=[OCTET], UserNum=[INTEGER], APID=[INTEGER])

The AP generates the alarm when the number of roaming users exceeds the alarm threshold.

Attribute

Alarm ID	Alarm Severity	Alarm Type
4287373448	Minor	equipmentAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
APMAC	Indicates the MAC address of an AP.
RadioID	Indicates the radio ID of the AP.
APName	Indicates the AP name.
UserNum	Indicates the number of UAC users.
APID	Indicates the AP ID.

Impact on the System

New users cannot roam to the AP.

Possible Causes

The number of roaming users on the AP exceeds the alarm threshold.

Procedure

Step 1 Run the **uac client-number threshold threshold access access-threshold [roam roam-threshold]** command in the radio profile view to increase the upper limit on the number of roaming users. Then, check whether the alarm persists.

- If so, go to Step 2.
- If not, go to Step 3.

Step 2 Collect alarm messages, log messages, and configurations, and then contact the technical support personnel.

Step 3 End.

----End

Related Information

None

3.4.170 ALM-303046771 AP roam user number exceed threshold notify

Description

WLAN/4/ROAM_STA_NUM_EXCEED_THRESHOLD_RESTORE:OID [OID] AP roam user number exceed threshold notify restore. (APMAC=[OPAQUE], RadioID=[INTEGER], APName=[OCTET], UserNum=[INTEGER], APID=[INTEGER])

The AP generates the alarm clearance notification when the number of roaming users falls below the alarm threshold.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046771	Warning	equipmentAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
APMAC	Indicates the MAC address of an AP.
RadioID	Indicates the radio ID of the AP.

Name	Meaning
APName	Indicates the AP name.
UserNum	Indicates the number of UAC users.
APID	Indicates the AP ID.

Impact on the System

None

Possible Causes

The number of roaming users falls below the alarm threshold.

Procedure

Step 1 This alarm is informational only, and no action is required.

----End

Related Information

None

3.4.171 ALM-303046704 AP Access Channel Utilization Exceeds the Threshold

Description

WLAN/4/CHANNEL_UTIL_EXCEED_THRESHOLD:OID [OID] AP access channel utilization exceed threshold notify. (APMAC=[OPAQUE], RadiolD=[INTEGER], APName=[OCTET],ChannelUtil=[INTEGER], APID=[INTEGER])

The AP generates the alarm when the channel usage exceeds the alarm threshold.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046704	Warning	equipmentAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.

Name	Meaning
APMAC	Indicates the MAC address of an AP.
APName	Indicates the AP name.
RadioID	Indicates the radio ID of the AP.
ChannelUtil	Indicates the channel usage.
APID	Indicates the AP ID.

Impact on the System

New users cannot access the network.

Possible Causes

The channel usage exceeds the alarm threshold when users associate with the AP.

Procedure

- Step 1

Run the **uac channel-utilization threshold threshold access** *access-threshold* [**roam** *roam-threshold*] command in the radio profile view to increase the upper limit on the number of users. Then, check whether the alarm persists.

- If so, go to Step 2.
 - If not, go to Step 3.
- Step 2

Collect alarm messages, log messages, and configurations, and then contact the technical support personnel.
- Step 3

End.
- End

Related Information

None

3.4.172 ALM-303046781 The Channel Usage by Roaming STAs Exceeds the Alarm Threshold

Description

WLAN/4/ROAM_CHANNEL_UTIL_EXCEED_THRESHOLD:OID [OID] AP roam channel utilization exceed threshold notify. (APMAC=[OPAQUE], RadioID=[INTEGER], APName=[OCTET],ChannelUtil=[INTEGER], APID=[INTEGER])

The AP generates the alarm when the channel usage by roaming STAs exceeds the alarm threshold.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046781	Warning	equipmentAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
APMAC	Indicates the MAC address of an AP.
RadioID	Indicates the radio ID of the AP.
APName	Indicates the AP name.
ChannelUtil	Indicates the channel usage.
APID	Indicates the AP ID.

Impact on the System

New users cannot roam to the AP.

Possible Causes

The channel usage exceeds the alarm threshold when users roam to the AP.

Procedure

- Step 1

Run the **uac channel-utilization threshold threshold access** *access-threshold* [**roam** *roam-threshold*] command in the radio profile view to increase the upper limit on the number of roaming users. Then, check whether the alarm persists.

- If so, go to Step 2.
 - If not, go to Step 3.
- Step 2

Collect alarm messages, log messages, and configurations, and then contact the technical support personnel.
- Step 3

End.
- End

Related Information

None

3.4.173 ALM-303046766 RADIO reach the max number of stations notify

Description

WLAN/4/RADIO_REACH_MAX_USER_PHY_SPECS:OID [OID] RADIO reach the max number of stations notify.(APMAC=[OPAQUE], RADIOID=[INTEGER], APID=[INTEGER], APName=[STRING], StaNum=[INTEGER], MaxStaNum=[INTEGER])

The number of access STAs reached the maximum physical specifications supported by a radio.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046766	Warning	equipmentAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object of the alarm.
APMAC	Indicates the MAC address of an AP.
RADIOID	Indicates the radio ID.
APID	Indicates the AP ID.
APName	Indicates the AP name.
StaNum	Indicates the number of access STAs.
MaxStaNum	Indicates the maximum number of access STAs supported by the radio.

Impact on the System

New STAs cannot go online.

Possible Causes

The number of access STAs reached the maximum physical specifications supported by a radio.

Procedure

- Step 1** Replace the AP with a model supporting more access STAs or expand the AP capacity.

- If the alarm persists, go to step 2.
- If the alarm is cleared, go to step 3.

Step 2 Collect alarms, logs, and configurations, and then contact technical support personnel.

Step 3 End.

----End

Related Information

None

3.4.174 ALM-303046759 The number of VAP instances has exceeded the maximum

Description

WLAN/2/VAP_NUM_EXCEEDED: OID [OID] The number of VAP instances has exceeded the maximum. (Vap = [INTEGER])

The number of VAP instances exceeds the maximum specifications of the system.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046759	Major	event

Parameters

Name	Meaning
OID	Indicates the MIB object of the alarm.
Vap	Indicates the maximum number of VAPs.

Impact on the System

VAPs that exceed the specifications cannot be created.

Possible Causes

The number of VAP instances reaches the maximum specifications of the system.

Procedure

- Step 1** Run the **display vap all** command to view all VAPs on the device.
- Step 2** Run the **display ap by-ssid** *ssid* command to view information about an AP group with a specified SSID.
- Step 3** Run the **ap-group name** *group-name* command to enter the AP group view.
- Step 4** Run the **undo vap-profile** *profile-name* **wlan** *wlan-id* { **radio** { *radio-id* | **all** } } command to delete one or more VAPs that are not needed.
- If the alarm persists, go to Step 5.
 - If the alarm is cleared, go to Step 7.
- Step 5** Collect alarm messages, log messages, and configurations, and then contact the technical support personnel.
- Step 6** End.
- End

Related Information

None

3.4.175 ALM-303046760 The IGMP snooping bandwidth of VAP has reached the maximum

Description

WLAN/4/VAP_IGMP_SNOOPING_BANDWIDTH_EXCEEDED: OID [OID] The IGMP snooping bandwidth of VAP has reached the maximum. (APMAC=[OPAQUE], RADIOID=[INTEGER], WLANID=[INTEGER], APName=[STRING], MaxBandWidth=[INTEGER], APID=[INTEGER])

The multicast bandwidth of a VAP exceeds the threshold.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046760	Warning	Quality of service alarm

Parameters

Name	Meaning
OID	ID of a MIB object.
APMAC	MAC address of an AP.
RADIOID	Radio ID.

Name	Meaning
WLANID	WLAN ID.
APName	AP name.
MaxBandWidth	Maximum multicast bandwidth of a VAP.
APID	AP ID.

Impact on the System

New users cannot join multicast groups.

Possible Causes

The multicast traffic of the VAP exceeds the maximum multicast bandwidth configured for the VAP.

Procedure

- Step 1** Run the **display traffic-profile { all | name *profile-name* }** command to check whether the maximum multicast bandwidth of a VAP is properly configured.
- If so, the actual multicast traffic is too large, and it is normal that users are prevented from joining multicast groups, and no action is required. Go to Step 5.
 - If not, go to Step 2.
- Step 2** Run the **igmp-snooping max-bandwidth *max-bandwidth*** command to configure a large value for the maximum multicast bandwidth of a VAP.
- Step 3** Check whether the alarm persists.
- If so, go to Step 4.
 - If not, go to Step 5.
- Step 4** Collect trap, log, and configuration information, and contact technical support personnel.
- Step 5** End.
- End

Related Information

None

3.4.176 ALM-303046761 The IGMP Snooping User of VAP Has Reached the Threshold

Description

WLAN/4/VAP_IGMP_SNOOPING_USER_EXCEEDED: OID [oid] The IGMP snooping user of VAP has reached the maximum. (APMAC=[OPAQUE], RADIOID=[INTEGER], WLANID=[INTEGER], APName=[STRING], MaxUserNum=[INTEGER], APID=[INTEGER])

The number of multicast bandwidth memberships on a VAP exceeds the threshold.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046761	Warning	Quality of service alarm

Parameters

Name	Meaning
OID	ID of a MIB object.
APMAC	MAC address of an AP.
RADIOID	Radio ID.
WLANID	WLAN ID.
APName	AP name.
MaxUserNum	Maximum number of multicast group memberships on a VAP.
APID	AP ID.

Impact on the System

New users cannot join multicast groups.

Possible Causes

The number of multicast users on the VAP exceeds the maximum number of multicast group memberships configured for the VAP.

Procedure

- Step 1** Run the **display traffic-profile { all | name *profile-name* }** command to check whether the maximum number of multicast group memberships on the VAP is properly configured.

- If so, the actual multicast traffic is too large, and it is normal that users are prevented from joining multicast groups, and no action is required. Go to step 5.
- If not, go to step 2.

Step 2 Run the **igmp-snooping max-user** *max-user* command to set a large value for the maximum number of multicast group memberships on the VAP.

Step 3 Check whether the alarm persists.

- If so, go to step 4.
- If not, go to step 5.

Step 4 Collect trap, log, and configuration information, and contact technical support personnel.

Step 5 End.

----End

Related Information

None

3.4.177 ALM-303046763 A VAP Fails to Be Created

Description

WLAN/4/VAP_CREATE_FAIL: OID [OID] VAP create fail.(Reason=[STRING])

A VAP fails to be created.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046763	Warning	equipmentAlarm

Parameters

Name	Meaning
Reason	Indicates the reason for the failure to create a VAP.

Impact on the System

The VAP cannot be created.

Possible Causes

Table 3-1 Reasons for VAP creation failures

Reason for VAP Creation Failures	Remarks	Suggestion
The VAPs using WEP encryption on an AP cannot use the same key ID.	-	Check the configuration of the VAP profile or security profile.
Invalid WEP key index.	-	Check whether the security profile is configured correctly.
Preshared key is not configured.	-	Configure a pre-shared key.
Only one management VAP profile can be bound.	-	Delete the management VAP that has been configured.
The bridge is enabled. Please undo first.	WLAN IDs 13 and 14 are used to set up a WDS bridge. Select other WLAN IDs or delete the WDS configuration.	Select another WLAN ID or delete the WDS configuration.
WLAN ID(16) is used. Please undo first.	WLAN ID 16 is used to set up a Mesh link. Select another WLAN ID or delete the Mesh configuration.	Select another WLAN ID or delete the Mesh configuration.
Only one temporary management vap-profile can be bound to an AP.	-	Delete the offline management VAP that has been configured.
The current country code does not support 5GHz frequency band.	-	Change the country code, or do not create a 5 GHz VAP.
The current country code does not support 2.4GHz frequency band.	-	Change the country code, or do not create a 2.4 GHz VAP.
The AP type does not support the wlan id.	-	Delete unused VAPs.
This AP type does not support WDS function.	-	Replace the AP with one supporting WDS.
This AP type does not support Mesh function.	-	Replace the AP with one supporting Mesh.

Reason for VAP Creation Failures	Remarks	Suggestion
This AP type or version does not support Mesh function.	-	Replace the AP with a Mesh-capable AP or upgrade the AP to a Mesh-capable version.
The number of VAPs has reached the upper limit.	-	Delete excess VAPs.
The AP does not support 5GHz frequency band.	-	Change the AP, or do not create a 5 GHz VAP.
The AP does not support 2.4GHz frequency band.	-	Change the AP, or do not create a 2.4 GHz VAP.
The AP does not support 802.1X+WEP.	-	Replace the AP with one in compliance with 802.11ac Wave 2.
SFN roaming can be configured only on one VAP of each radio.	-	Create a VAP on another radio or delete the SFN roaming VAP on the current radio.
The AP does not support SFN.	-	Replace the AP with one supporting SFN roaming.
The 5G radio of the AP does not support SFN.	-	Replace the AP or change the 5 GHz radio configuration.
The number of VAPs has reached the card specific.	-	Reduce the number of VAPs on a card, or enable the AP to go online on another card of the switch and create VAPs.
The AP in this version does not support PPSK authentication.	-	Upgrade the AP to V200R010C00 or later.
The AP in this version does not support Navi-AC VAPs.	-	Upgrade the AP to V200R010C00 or later.
Unknown reason, error code is 0x%x.	-	Contact technical support personnel.
The number of WDS VAPs has reached the upper limit.	-	Delete redundant WDS VAPs.

Reason for VAP Creation Failures	Remarks	Suggestion
The number of Mesh VAPs has reached the upper limit.	-	Delete redundant Mesh VAPs.
The frequency band of this radio is inconsistent with that supported by the current country code.	-	Change the country code, or do not create a VAP for the current radio.
The AP in this version does not support the Mesh configuration on radio 2.	-	Upgrade APs to V200R020C10 or later.
The AP does not support OWE.	-	Upgrade APs to V200R020C10 or later.

Procedure

Step 1 Handling the alarm based on different reasons. For detailed handling suggestions, see Table 2.

----End

Related Information

None

3.4.178 ALM-303046767 Station author is error notify

Description

WLAN/4/STA_AUTH_FAIL: OID [oid] Station author is error notify.
(APMAC=[OPAQUE],APMAC=[OPAQUE],RadioID=[INTEGER],StaMac=[OPAQUE],APName=[OCTET],StaAssocBssid=[OPAQUE],Ssid=[OCTET],StaAuthenticationMode=[INTEGER],StaFailCodeType=[OCTET],StaAuthenticationFailCause=[INTEGER],StaAuthenticationFailCauseStr=[OCTET], APID=[INTEGER])

A STA failed to be authenticated.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046767	Warning	equipmentAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
APMAC	Indicates the MAC address of an AP.
RadioID	Indicates the radio ID.
StaMac	Indicates the MAC address of a STA, which identifies the STA and functions as the index for querying information associated with the STA.
APName	Indicates the AP name.
StaAssocBssid	Indicates the BSSID associated with the STA.
Ssid	Indicates the SSID associated with the STA.
StaAuthenticationMode	Indicates the authentication mode of the STA.
StaFailCodeType	Indicates the code type of failures of STA authentication and association. • 1: Reason code • 2: Status code
StaAuthenticationFailCause	Indicates the index of the authentication failure reason.
StaAuthenticationFailCauseStr	Indicates the user authentication failure reason.
APID	Indicates the AP ID.

Impact on the System

STAs cannot go online.

Possible Causes

The AP was configured with the WEP shared key authentication mode and the STA sent a connection request with an incorrect password.

Procedure

- Step 1** Check whether the shared key is configured correctly.
- If so, go to Step 2.

- If not, this is a common event. Go to step 3.

Step 2 Collect alarm messages, log messages, and configurations, and then contact the technical support personnel.

Step 3 End.

----End

Related Information

None

3.4.179 ALM-303046768 Station association is failed notify

Description

WLAN/4/STA_ASSOCIATION_FAIL: OID [OID] Station association is failed notify.
(APMAC=[OPAQUE],APMAC=[OPAQUE],RadioID=[INTEGER],StaMac=[OPAQUE],APName=[OCTET],StaAssocBssid=[OPAQUE],Ssid=[OCTET],StaFailCodeType=[OCTET],StaAuthenticationFailCause=[INTEGER], StaAssociationFailCauseStr=[OCTET], APID=[INTEGER])

A STA failed to associate with the AP.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046768	Warning	equipmentAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
APMAC	Indicates the MAC address of an AP.
RadioID	Indicates the radio ID.
StaMac	Indicates the MAC address of a STA, which identifies the STA and functions as the index for querying information associated with the STA.
APName	Indicates the AP name.
StaAssocBssid	Indicates the BSSID associated with the STA.
Ssid	Indicates the SSID associated with the STA.

Name	Meaning
StaAuthenticationMode	Indicates the authentication mode of the STA.
StaFailCodeType	Indicates the code type of failures of STA authentication and association. • 1: Reason code • 2: Status code
StaAuthenticationFailCause	Indicates the index of the authentication failure reason.
StaAuthenticationFailCauseStr	Indicates the user authentication failure reason.
APID	Indicates the AP ID.

Impact on the System

STAs cannot go online.

Possible Causes

The number of STAs that send association requests to the AP exceeded the maximum value allowed by the AP.

Procedure

- Step 1** Run the **display sta-blacklist-profile** command to check whether the STA is in the specified STA blacklist profile.
- If so, go to Step 2.
 - If not, go to Step 3.
- Step 2** Run the **undo sta-mac** command to delete the STA from the blacklist. Check whether the alarm persists.
- If so, go to Step 3.
 - If not, go to Step 6.
- Step 3** Check whether the number of STAs has reached the allowed maximum value.
- If so, go to Step 4.
 - If not, go to Step 5.
- Step 4** Associate STAs with other APs. Check whether the alarm persists.
- If so, go to Step 5.
 - If not, go to Step 6.
- Step 5** Collect alarm messages, log messages, and configurations, and then contact the technical support personnel.

Step 6 End.
----End

Related Information

None

3.4.180 ALM-303046969 A User with an Invalid Certificate Accessed the Network

Description

WLAN/4/STA_INVALID_CERT_ATTACK: OID [OID] User with invalid cerfication inbreak network notify.
(APMAC=[OPAQUE],APMAC=[OPAQUE],RadioID=[INTEGER],StaMac=[OPAQUE],APName=[OCTET],StaAssocBssid=[OPAQUE],Ssid=[OCTET], APID=[INTEGER])
A user with an invalid certificate accessed the network.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046969	Warning	equipmentAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
APMAC	Indicates the MAC address of an AP.
RadioID	Indicates the radio ID.
StaMac	Indicates the MAC address of a STA, which identifies the STA and functions as the index for querying information associated with the STA.
APName	Indicates the AP name.
StaAssocBssid	Indicates the BSSID associated with the STA.
Ssid	Indicates the SSID associated with the STA.
APID	Indicates the AP ID.

Impact on the System

STAs cannot go online.

Possible Causes

A user with an invalid WAPI certificate accessed the network.

Procedure

- Step 1

Run the **display wlan wapi certificate file-name** *file-name* command to check whether the WAPI certificate is correct.
- If so, go to Step 3.
 - If not, go to Step 2.
- Step 2

Run the **wapi import certificate { ac | asu | issuer } format pkcs12 file-name** *file-name* **password** *password* or **wapi import certificate { ac | asu | issuer } format pem file-name** *file-name* command to import a correct WAPI certificate. Check whether the alarm persists.
- If so, go to Step 3.
 - If not, go to Step 4.
- Step 3

Collect alarm messages, log messages, and configurations, and then contact the technical support personnel.
- Step 4

End.
- End

Related Information

None

3.4.181 ALM-303046976 An STA Was Attacked by Replay Attacks

Description

WLAN/4/STA_REPLAY_ATTACK:OID [oid] Station repitive attack notify.
(APMAC=[OPAQUE],APMAC=[OPAQUE],RadioID=[INTEGER],StaMac=[OPAQUE],APName=[OCTET],StaAssocBssid=[OPAQUE],Ssid=[OCTET], APID=[INTEGER])

The STA was attacked by replay attacks.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046976	Warning	equipmentAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
APMAC	Indicates the MAC address of an AP.
RadioID	Indicates the radio ID.
StaMac	Indicates the MAC address of a STA, which identifies the STA and functions as the index for querying information associated with the STA.
APName	Indicates the AP name.
StaAssocBssid	Indicates the BSSID associated with the STA.
Ssid	Indicates the SSID associated with the STA.
APID	Indicates the AP ID.

Impact on the System

STAs cannot go online.

Possible Causes

The AP received unauthorized AE questions.

Procedure

- Step 1** Check whether the MAC address of the STA is the same as that of the attack device.
- If so, go to Step 2.
 - If not, go to Step 4.
- Step 2** Run the **sta-mac mac-address [description description]** command to add the attack device's MAC address to the blacklist in the STA blacklist profile view.
- Step 3** Check whether the alarm persists.
- If so, go to Step 4.
 - If not, go to Step 5.
- Step 4** Collect alarm messages, log messages, and configurations, and then contact the technical support personnel.
- Step 5** End.
- End

Related Information

None

3.4.182 ALM-303046739 Tamper attack notify

Description

WLAN/4/STA_TAMPER_ATTACK: OID [OID] Tamper attack notify.
(APMAC=[OPAQUE],APMAC=[OPAQUE],RadioID=[INTEGER],StaMac=[OPAQUE],APName=[OCTET],StaAssocBssid=[OPAQUE],Ssid=[OCTET], APID=[INTEGER])

Attack messages were modified.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046739	Warning	equipmentAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
APMAC	Indicates the MAC address of an AP.
RadioID	Indicates the radio ID.
StaMac	Indicates the MAC address of a STA, which identifies the STA and functions as the index for querying information associated with the STA.
APName	Indicates the AP name.
StaAssocBssid	Indicates the BSSID associated with the STA.
Ssid	Indicates the SSID associated with the STA.
APID	Indicates the AP ID.

Impact on the System

STAs cannot go online.

Possible Causes

The AP received incorrect message authentication codes.

Procedure

- Step 1
Check whether the MAC address of the STA is the same as that of the attack device.
 - If so, go to Step 2.
 - If not, go to Step 4.
- Step 2
Run the `sta-mac mac-address [ description description ]` command to add the attack device's MAC address to the blacklist in the STA blacklist profile view.
- Step 3
Check whether the alarm persists.
 - If so, go to Step 4.
 - If not, go to Step 5.
- Step 4
Collect alarm messages, log messages, and configurations, and then contact the technical support personnel.
- Step 5
End.
- End

Related Information

None

3.4.183 ALM-303046740 The AP Security Level Was Lowered by Attacks

Description

WLAN/4/STA_SECURITY_CLASS_LOW_ATTACK: OID [oid] Low safelevel attack notify.

(APMAC=[OPAQUE],APMAC=[OPAQUE],RadioID=[INTEGER],StaMac=[OPAQUE],APName=[OCTET],StaAssocBssid=[OPAQUE],Ssid=[OCTET], APID=[INTEGER])

The AP security level was lowered by attacks.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046740	Warning	equipmentAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
APMAC	Indicates the MAC address of an AP.
RadioID	Indicates the radio ID.
StaMac	Indicates the MAC address of a STA, which identifies the STA and functions as the index for querying information associated with the STA.
APName	Indicates the AP name.
StaAssocBssid	Indicates the BSSID associated with the STA.
Ssid	Indicates the SSID associated with the STA.
APID	Indicates the AP ID.

Impact on the System

STAs cannot go online.

Possible Causes

The AP received key negotiation response packets with incorrect WIEASUE.

Procedure

- Step 1

Check whether the MAC address of the STA is the same as that of the attack device.
 - If so, go to Step 2.
 - If not, go to Step 4.
- Step 2

Run the `sta-mac mac-address [ description description ]` command to add the attack device's MAC address to the blacklist in the STA blacklist profile view.
- Step 3

Check whether the alarm persists.
 - If so, go to Step 4.
 - If not, go to Step 5.
- Step 4

Collect alarm messages, log messages, and configurations, and then contact the technical support personnel.
- Step 5

End.
- End

Related Information

None

3.4.184 ALM-303046741 Address redirection attack notify

Description

WLAN/4/STA_ADDRESS_REDIRCET_ATTACK:OID [OID] Address redirection attack notify.
(APMAC=[OPAQUE],APMAC=[OPAQUE],RadioID=[INTEGER],StaMac=[OPAQUE],APName=[OCTET],StaAssocBssid=[OPAQUE],Ssid=[OCTET], APID=[INTEGER])

An address redirection attack was detected.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046741	Warning	equipmentAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
APMAC	Indicates the MAC address of an AP.
RadioID	Indicates the radio ID.
StaMac	Indicates the MAC address of a STA, which identifies the STA and functions as the index for querying information associated with the STA.
APName	Indicates the AP name.
StaAssocBssid	Indicates the BSSID associated with the STA.
Ssid	Indicates the SSID associated with the STA.
APID	Indicates the AP ID.

Impact on the System

STAs cannot go online.

Possible Causes

The AP received invalid WPI frames.

Procedure

- Step 1
Check whether the MAC address of the STA is the same as that of the attack device.
 - If so, go to Step 2.
 - If not, go to Step 4.
- Step 2
Run the `sta-mac mac-address [ description description ]` command to add the attack device's MAC address to the blacklist in the STA blacklist profile view.
- Step 3
Check whether the alarm persists.
 - If so, go to Step 4.
 - If not, go to Step 5.
- Step 4
Collect alarm messages, log messages, and configurations, and then contact the technical support personnel.
- Step 5
End.
- End

Related Information

None

3.4.185 ALM-303046769 SSID WEP key conflict notify

Description

WLAN/4/SSID_CONFLICT_WEP_KEY:OID [OID] SSID Wep key conflict notify.
 (APMAC=[OPAQUE],WepIDConflictTrapAPMAC=[OPAQUE],WepIDConflictTrapAPName=[OCTET],WepIDConflictTrapRadioId=[INTEGER],WepIDConflictTrapPreSSID=[OCTET],WepIDConflictTrapCurrSSID=[OCTET],WepIDConflictTrapCipherIdx=[INTEGER], APID=[INTEGER])

WEP key ID collision has occurred.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046769	Warning	processingErrorAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
APMAC	Indicates the table index.
WepIDConflictTrapAPMAC	Indicates the MAC address of an AP.
WepIDConflictTrapAPName	Indicates the AP name.
WepIDConflictTrapRadioId	Indicates the radio ID configured on the AP when the collision happens.
WepIDConflictTrapPreSSID	Indicates the SSID configured before the collision.
WepIDConflictTrapCurrSSID	Indicates the SSID configured when the collision happens.
WepIDConflictTrapCipherIdx	Indicates the WEP key ID that causes the collision.
APID	Indicates the AP ID.

Impact on the System

Users fail to go online.

Possible Causes

Different WEP key IDs are configured in the security profiles bound to different VAPs.

Procedure

Step 1 Run the **wep key** command to change **key-id** in the security profiles.

- If the alarm persists, go to Step 2.
- If the alarm is cleared, go to Step 3.

Step 2 Collect alarm messages, log messages, and configurations, and then contact the technical support personnel.

Step 3 End.

----End

Related Information

None

3.4.186 ALM-303046988 The Local WAC Configuration Is Inconsistent with that on the Remote WAC

Description

WLAN/4/AC_CONFIG_MISMATCH:OID [OID] The local AC configuration is inconsistent with that on the remote AC. (RemoteAC=[IPADDR], Reason=[OCTET])

An alarm was generated when configurations of ACs were inconsistent after configuration synchronization.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046988	Major	equipmentAlarm

Parameters

Name	Meaning
OID	ID of a MIB object.
RemoteAC	IP address of the remote AC.
Reason	Reason for configuration inconsistency.

Impact on the System

The local AC or backup master AC cannot synchronize configurations from the master AC.

Possible Causes

The configurations of ACs are inconsistent after configuration synchronization.

Procedure

- Step 1** Run the **synchronize-configuration** command to manually enable wireless configuration synchronization. Check whether the alarm persists.
- If so, go to Step 2.
 - If not, go to Step 3.
- Step 2** Collect alarm, log, and configuration information, and contact Huawei technical support personnel.
- Step 3** End.
- End

Related Information

None

3.4.187 ALM-3416071 AP Power Supply Insufficient

Description

ENTITYTRAP/2/PWR_INSUFF:OID [OID] AP power supply is insufficient.
(PowerWorkMode=[OCTET], ExpectPowerWorkMode=[OCTET])

The AP power supply was insufficient.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3416071	Major	equipmentAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object of the alarm.
PowerWorkMode	Indicates the actual power supply mode of an AP.
ExpectPowerWorkMode	Indicates the expected power supply mode of an AP.

Impact on the System

The AP restarts due to insufficient power supply.

Possible Causes

The power supply is insufficient for the AP.

Procedure

- Step 1** Run the **lldp enable** command in the interface view to enable the LLDP function. In this way, the peer power supply device can identify the power supply standard of the local device and supply power as required.
- If the alarm persists, go to step 2.
 - If the alarm is cleared, go to step 4.
- Step 2** Check the peer power supply device and ensure that the power supply standard meets the AP's power supply requirements.

- If the alarm persists, go to step 3.
- If the alarm is cleared, go to step 4.

Step 3 Collect alarm and configuration information, and contact technical support personnel.

Step 4 End.

----End

Related Information

None

3.4.188 ALM-303046912 Disk usage exceeds the threshold

Description

MID_ENTITY_TRAP/4/TRAPID_ENTITY_DISK_UTILIZATION_RISING:OID [OID]
Storage utilization exceeded the pre-alarm threshold.
(HwEntityPhysicalIndex=[INTEGER], PhysicalName=\"[OCTET]\",
EntityThresholdType=[INTEGER], EntityThresholdWarning=[INTEGER],
EntityThresholdCurrent=[INTEGER], EntityTrapFaultID=[INTEGER])

The disk usage exceeds the upper alarm threshold.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046912	Warning	equipmentAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object of the alarm.
HwEntityPhysicalIndex	Indicates the physical entity index.
PhysicalName	Indicates the physical entity name.
EntityThresholdType	Indicates the threshold type.
EntityThresholdWarning	Indicates the alarm threshold.
EntityThresholdCurrent	Indicates the current value.
EntityTrapFaultID	Error Code

Impact on the System

The configuration may fail to be saved.

Possible Causes

The AP's disk space is fully occupied.

Procedure

Step 1 Run the **dir** command in the user view to check files in the system.

Step 2 Run the **delete [/unreserved]** command to delete unnecessary files.

Files that can be deleted include those that are saved by the user and generated using commands, as well as the following in the system inventory:

- **logfile**: stores log files, which can be exported and then deleted.
- **corefile**: stores exception information files, which can be exported and then deleted.

Step 3 Collect alarms, logs, and configurations, and then contact technical support personnel.

Step 4 End.

----End

3.4.189 ALM-303046764 AP has the max number of stations notify

Description

WLAN/4/AP_REACH_MAX_USERS:OID [OID] AP has the max number of stations notify.(APMAC=[OPAQUE], APName=[STRING], FailCause=[INTEGER], PermitNum=[INTEGER], APID=[INTEGER])

The maximum number of STAs associated with the AP was reached.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046764	Warning	equipmentAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.

Name	Meaning
APMAC	Indicates the MAC address of an AP.
APName	Indicates the AP name.
FailCause	Indicates the cause for the STA authentication failure.
PermitNum	Indicates the maximum number of STAs that can be associated with the AP.
APID	Indicates the AP ID.

Impact on the System

The newly added STAs cannot go online.

Possible Causes

The number of STAs connected to an AP has reached the upper limit. New STAs cannot connect to the VAP.

Procedure

Step 1 Re-plan the network and increase the network capacity.

----End

Related Information

None

3.4.190 ALM-3416072 AP broadcast and multicast packets over threshold.

Description

WLAN/4/MCBC_EXCEED:OID [OID] The number of multicast and broadcast packets received on the AP exceeds the threshold 1000 pps for 10 seconds. (APMAC=[OPAQUE], APName=[STRING], APID=[INTEGER])

The number of multicast and broadcast packets received by an AP exceeded the alarm threshold.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3416072	Warning	Quality of service alarm

Parameters

Name	Meaning
OID	Indicates the ID of the alarm MIB object.
APMAC	Indicates the MAC address of an AP.
APName	Indicates the AP name.
APID	Indicates the AP ID.

Impact on the System

If an AP receives too many multicast and broadcast packets, AP services are affected.

Possible Causes

The number of multicast and broadcast packets received by the AP exceeded the alarm threshold.

Procedure

- Step 1** Check the networking, find senders of the multicast and broadcast packets, and optimize the networking. Check whether the alarm persists.
- If so, go to Step 2.
 - If not, go to Step 4.
- Step 2** Run the **traffic-optimize broadcast-suppression enable** command in the system profile to enable the rate limit for broadcast packets and IGMP multicast packets on the AP. Check whether the alarm persists.
- If so, go to Step 3.
 - If not, go to Step 4.
- Step 3** Collect alarm, log, and configuration information, and contact technical support personnel.
- Step 4** End.
- End

3.4.191 ALM-3276800205 The IoT Card Is Disconnected from the Server

Description

WLAN/2/IOT_CARD_DISCONNECT_SERVER:OID [OID] The IoT card is disconnected from the server. (APMAC=[OPAQUE], APName=[STRING], APID=[INTEGER], AplotCardId=[INTEGER], AplotCardType=[STRING])

An IoT card is disconnected from the server.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800205	Major	equipmentAlarm

Parameters

Name	Meaning
OID	Indicates the ID of a MIB object.
APMAC	Indicates the MAC address of an AP.
APName	Indicates the AP name.
APID	Indicates the AP ID.
APlotCardId	Indicates the ID of an IoT card.
APlotCardType	Indicates the type of an IoT card.

Impact on the System

An IoT card cannot communicate with the server.

Possible Causes

Cause 1: The link between the IoT card and server is disconnected, or the network configuration changes.

Cause 2: The IoT card is faulty.

Procedure

- Step 1** Check whether the network configuration between the IoT card and server is normal.
- If so, go to Step 3.
 - If not, go to Step 2.
- Step 2** Correct the network configuration and check whether the alarm is cleared.
- If so, go to Step 5.
 - If not, go to Step 3.
- Step 3** Replace the IoT card and check whether the alarm is cleared.
- If so, go to Step 5.
 - If not, go to Step 4.

Step 4 Collect alarm and configuration information, and contact technical support personnel.

Step 5 End.

----End

Related Information

None

3.4.192 ALM-3276800206 The IoT card does not match the configured type

Description

WLAN/2/IOT_CARD_TYPE_MISMATCH:OID [OID] The IoT card does not match the configured type. (APMAC=[OPAQUE], APName=[STRING], APID=[INTEGER], APlotCardId=[INTEGER], APlotCardType=[STRING])

The IoT card type does not match the configuration.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800206	Major	equipmentAlarm

Parameters

Name	Meaning
OID	Indicates the ID of a MIB object.
APMAC	Indicates the MAC address of an AP.
APName	Indicates the AP name.
APID	Indicates the AP ID.
APlotCardId	Indicates the ID of an IoT card.
APlotCardType	Indicates the type of an IoT card.

Impact on the System

The AP cannot communicate with the IoT card.

Possible Causes

Cause 1: The configured IoT card type is incorrect.

Cause 2: The type of the inserted IoT card is incorrect.

Procedure

- Step 1** Check whether the IoT card type is correctly configured.
- If so, go to Step 3.
 - If not, go to Step 2.
- Step 2** Run the **card connect-type { ethernet | serial }** command to correctly configure the IoT card type. Check whether the alarm is cleared.
- If so, go to Step 5.
 - If not, go to Step 3.
- Step 3** Replace the IoT card with one of the correct type and check whether the alarm is cleared.
- If so, go to Step 5.
 - If not, go to Step 4.
- Step 4** Collect alarm and configuration information, and contact technical support personnel.
- Step 5** End.
- End

Related Information

None

3.4.193 ALM-303046411 The WAPI certificate is nearly expired

Description

WLAN/4/WAPI_CERT_NEARLY_EXPIRED: OID [OID] The WAPI certificate is nearly expired. (SecurityProfileName=[STRING], CertType=[STRING], CertFileName=[STRING], CertStartTime=[STRING], CertEndTime=[STRING])

The validity period of the WAPI certificate loaded to the security profile is less than 30 days.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046411	Warning	Quality of service alarm

Parameters

Name	Meaning
OID	Indicates the ID of a MIB object.
SecurityProfileName	Indicates the name of a security profile.
CertType	Indicates the type of a certificate. The value can be: • ac • asu • issuer
CertFileName	Indicates the name of a WAPI certificate file.
CertStartTime	Indicates the start time of WAPI certificate validity.
CertEndTime	Indicates the end time of WAPI certificate validity.

Impact on the System

After the WAPI certificate expires, users using this certificate cannot access the network.

Possible Causes

The validity period of the WAPI certificate loaded to the security profile is less than 30 days.

Procedure

Step 1 Check whether the current system time is correct.

- If so, go to step 3.
- If not, go to step 2.

Step 2 Change the system time.

- If the alarm persists, go to step 3.
- If the alarm is cleared, go to step 5.

Step 3 Replace the certificate before it expires.

- If the alarm persists, go to step 4.
- If the alarm is cleared, go to step 5.

Step 4 Collect alarm, log, and configuration information, and contact technical support personnel.

Step 5 End.
----End

Related Information

None

3.4.194 ALM-303046412 The WAPI certificate is invalid

Description

WLAN/2/WAPI_CERT_INVALID: OID [OID] The WAPI certificate is invalid.
(SecurityProfileName=[STRING], CertType=[STRING], CertFileName=[STRING],
CertStartTime=[STRING], CertEndTime=[STRING])

The WAPI certificate loaded to the security profile expires.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046412	Major	Quality of service alarm

Parameters

Name	Meaning
OID	Indicates the ID of a MIB object.
SecurityProfileName	Indicates the name of a security profile.
CertType	Indicates the type of a certificate. The value can be: - ac - asu - issuer
CertFileName	Indicates the name of a WAPI certificate file.
CertStartTime	Indicates the start time of WAPI certificate validity.
CertEndTime	Indicates the end time of WAPI certificate validity.

Impact on the System

Users using this certificate cannot access the network.

Possible Causes

The WAPI certificate loaded to the security profile expires.

Procedure

- Step 1** Check whether the current system time is correct.
- If so, go to step 3.
 - If not, go to step 2.
- Step 2** Change the system time.
- If the alarm persists, go to step 3.
 - If the alarm is cleared, go to step 5.
- Step 3** Replace the certificate.
- If the alarm persists, go to step 4.
 - If the alarm is cleared, go to step 5.
- Step 4** Collect alarm, log, and configuration information, and contact technical support personnel.
- Step 5** End.
- End

Related Information

None

3.4.195 ALM-303046413 The CA certificate is invalid

Description

PKI/2/PKICACERTINVALID: OID [OID] the CA certificate is invalid.
(CACertIssuer=[issuer], CACertSubject=[subject], CACertStartTime=[starttime], CACertFinishTime=[finishtime])

The CA certificate is invalid.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046413	Warning	Communication alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.

Name	Meaning
issuer	Indicates the issuer of the CA certificate.
subject	Indicates the subject of the CA certificate.
starttime	Indicates the start time of the CA certificate.
finishtime	Indicates the end time of the CA certificate.

Impact on the System

The service becomes invalid.

Possible Causes

The CA certificate is invalid.

Procedure

Step 1 Run the **display clock** command to check whether the device time is correct.

If not, run the **clock datetime** command in the user view to change the device time.

Step 2 Apply for a new certificate through SCEP or CMPv2 online or apply for a new certificate offline. For details, see the *Wireless Access Controller (AC and Fit AP) V200R019C00 Configuration Guide - PKI Configuration*.

----End

Related Information

None

3.4.196 ALM-303046414 The CA Certificate Is About to Expire

Description

PKI/4/PKICACERTNEARLYEXPIRED: OID [OID] the CA certificate is nearly expired. (CACertIssuer=[issuer], CACertSubject=[subject], CACertStartTime=[starttime], CACertFinishTime=[finishtime])

The CA certificate is about to expire.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046414	Warning	Communication alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
issuer	Indicates the issuer of the CA certificate.
subject	Indicates the subject of the CA certificate.
starttime	Indicates the start time of the CA certificate.
finishtime	Indicates the end time of the CA certificate.

Impact on the System

The service will be invalid after the certificate expires.

Possible Causes

The CA certificate is about to expire. The CA certificate expiration time is less than the certificate expired prewarning time configured by the **pki set-certificate expire-prewarning** command.

Procedure

Step 1 Run the **display clock** command to check whether the device time is correct.

If not, run the **clock datetime** command in the user view to change the device time.

Step 2 Apply for a new certificate through SCEP or CMPv2 online or apply for a new certificate offline. For details, see the *Wireless Access Controller (AC and FITAP) V200R019C00 Configuration Guide - PKI Configuration*.

----End

Related Information

None

3.4.197 ALM-303046415 The local certificate is invalid

Description

PKI/2/PKILOCALCERTINVALID: OID [OID] the local certificate is invalid.
(LocalCertIssuer=[issuer], LocalCertSubject=[subject],
LocalCertStartTime=[starttime], LocalCertFinishTime=[finishtime])

The local certificate is invalid.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046415	Warning	Communication alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
issuer	Indicates the issuer of the CA certificate.
subject	Indicates the subject of the CA certificate.
starttime	Indicates the start time of the CA certificate.
finishtime	Indicates the end time of the CA certificate.

Impact on the System

The service becomes invalid.

Possible Causes

The local certificate is invalid.

Procedure

Step 1 Check whether the system time on the local device is correct.

Step 2 If the system time is correct, apply for a new local certificate.

----End

Related Information

None

3.4.198 ALM-303046416 The local certificate is nearly expired

Description

PKI/4/PKILOCALCERTNEARLYEXPIRED: OID [OID] the local certificate is nearly expired. (LocalCertIssuer=[issuer], LocalCertSubject=[subject], LocalCertStartTime=[starttime], LocalCertFinishTime=[finishtime])

The local certificate is about to expire.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046416	Warning	Communication alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
issuer	Indicates the issuer of the CA certificate.
subject	Indicates the subject of the CA certificate.
starttime	Indicates the start time of the CA certificate.
finishtime	Indicates the end time of the CA certificate.

Impact on the System

The service will be invalid after the certificate expires.

Possible Causes

The local certificate is about to expire. The local certificate expiration time is less than the certificate expired prewarning time configured by the **pki set-certificate expire-prewarning** command.

Procedure

- Step 1** Check whether the system time on the local device is correct.
- Step 2** If the system time is correct, apply for a new local certificate immediately.
- End

Related Information

None

3.4.199 ALM-3276800218 System Rollback

Description

ENTITYTRAP/4/SYSTEMROLL:OID [OID] System rollback.
(Reason=[INTEGER],Version ="[OCTET]",FileName="[OCTET]")

If the specified startup software fails when you upgrade the system software or restart the device, the system will use the software that works last time. This alarm is generated when the startup succeeds, indicating that a version rollback occurs.

If the startup fails, the system will use the specified backup software. This alarm is generated when the startup succeeds, indicating that a version rollback occurs.

Attribute

Alarm ID	Alarm Severity	Alarm Type
3276800218	Warning	processingErrorAlarm

Parameters

Name	Meaning
OID	Indicates the ID of the MIB object.
Reason	Indicates the error code.
Version	Indicates the version before the rollback.
FileName	Indicates the file name.

Impact on the System

The system software supports only the service features of the current version after the startup succeeds.

Possible Causes

Rollback occurs on the system.

Procedure

- Step 1** Run the **dir** command to check the file system.
- If the storage medium is unavailable, the storage medium is corrupted. Go to step 2.
 - If the software that fails to start the system is in the file system, check the file size. If the file size is not in the allowed range, the system software is invalid. Go to step 3.
 - If the storage medium is available and the file size is within the allowed range, system software is faulty and cannot start the system. Go to step 4.
- Step 2** Check the storage medium saved in the system software.
- If the storage medium is an SD card or a USB disk, replace it and restart the upgrade. If the upgrade fails, go to step 4.
 - If the storage medium is flash, record the device type and number and contact technical support personnel.
- Step 3** Delete the invalid file and upload a complete file. Perform the upgrade. If the upgrade fails, go to step 4.
- Step 4** Collect operation results and contact technical support personnel.
- Step 5** If the system time is correct, apply for a new local certificate immediately.
- End

Related Information

None

3.4.200 ALM-303046417 Session resources exceed the threshold

Description

ENTITYTRAP/6/AP_SESSION_EXCEEDS_THRESHOLD:OID [OID] The AP session usage exceeds the threshold.(ApSessionNum=[INTEGER], ApSessionNumThreshold=[INTEGER],ApSessionNumSpec = [INTEGER].)

Session resources exceed the threshold.

Attribute

Alarm ID	Alarm Severity	Alarm Type
303046417	Warning	equipmentAlarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
ApSessionNum	Indicates AP session number.
ApSessionNumThreshold	Indicates the threshold of AP session number.
ApSessionNumSpec	Indicates the specification of AP session number.

Impact on the System

When session resources are insufficient, the communication between the AP and iMaster NCE and Internet access services are affected. When session resources are exhausted, user services or AP services are affected.

Possible Causes

Frequent link establishment for the STA or AP services occupy a large number of resources, which are not released in a timely manner.

Procedure

Step 1 Run the **display diagnostic-information saved-file saved-info.txt** command to collect local information on the device.

Step 2 Send the collected information to the technical support personnel.

----End

Related Information

None

3.4.201 ALM-1707675682 Container CPU utilization is greater than the alarm threshold

Description

ENTITYTRAP/2/CONTAINERCPURISE: "OID [oid] Container CPU utilization exceeded the pre-alarm threshold.(Index=[INTEGER], HwEntityPhysicalIndex=[INTEGER], PhysicalName="[OCTET]", ContainerName="[OCTET]", EntityThresholdType=[INTEGER], EntityThresholdWarning=[INTEGER], EntityThresholdCurrent=[INTEGER], EntityTrapFaultID=[INTEGER])"

The CPU usage of the container exceeds the alarm threshold.

 NOTE

Only cloud APs support this alarm.

Attribute

Alarm ID	Alarm OID	Alarm Severity	Alarm Type
1707675682	1.3.6.1.4.1.2011.5.25.219.2.42.1	Major	equipmentAlarm

Parameters

Name	Meaning
OID	Indicates the ID of a MIB object.
Index	Indicates the entity index.
HwEntityPhysicalIndex	Indicates the physical entity index.
PhysicalName	Indicates the physical entity name.
ContainerName	Indicates the container name.
EntityThresholdType	Indicates the threshold type.
EntityThresholdWarning	Indicates the alarm threshold.
EntityThresholdCurrent	Indicates the current value.
EntityTrapFaultID	Indicates the error code.

Impact on the System

The container and applications in the container cannot run properly.

Possible Causes

The container or an application in the container is not running properly. As a result, the CPU usage of the container exceeds 90% for 120 consecutive seconds.

Procedure

- Step 1** Run the **display container information** command to check the status of the container.

Step 2 Collect alarm messages, log messages, configurations, and container status information collected in step 1, and contact technical support personnel.

Step 3 End.

----End

3.4.202 ALM-1707675683 Container memory usage above threshold

Description

ENTITYTRAP/2/CONTAINERMEMRISE: "OID [oid] Container memory utilization exceeded the pre-alarm threshold.(Index=[INTEGER], HwEntityPhysicalIndex=[INTEGER], PhysicalName="[OCTET]", ContainerName="[OCTET]", EntityThresholdType=[INTEGER], EntityThresholdWarning=[INTEGER], EntityThresholdCurrent=[INTEGER], EntityTrapFaultID=[INTEGER])"

The memory usage of the container exceeds the alarm threshold.

Attribute

Alarm ID	Alarm OID	Alarm Severity	Alarm Type
1707675683	1.3.6.1.4.1.2011.5.25.219.2.42.3	Major	equipmentAlarm

Parameters

Name	Meaning
OID	Indicates the ID of a MIB object.
Index	Indicates the entity index.
HwEntityPhysicalIndex	Indicates the physical entity index.
PhysicalName	Indicates the physical entity name.
ContainerName	Indicates the container name.
EntityThresholdType	Indicates the threshold type.
EntityThresholdWarning	Indicates the alarm threshold.
EntityThresholdCurrent	Indicates the current value.

Name	Meaning
EntityTrapFaultID	Indicates the error code.

Impact on the System

The container and applications in the container cannot run properly.

Possible Causes

The container or an application in the container is not running properly. As a result, the memory usage of the container exceeds 95% for 60 consecutive seconds.

Procedure

- Step 1** Run the **display container information** command to check the status of the container.
- Step 2** Collect alarm messages, log messages, configurations, and container status information collected in step 1, and contact technical support personnel.
- Step 3** End.

----End

3.4.203 ALM-1707675684 Container storage space utilization too high alarm

Description

ENTITYTRAP/2/CONTAINERSTORAGERISE: "OID [oid] Container storage utilization exceeded the pre-alarm threshold.(Index=[INTEGER], HwEntityPhysicalIndex=[INTEGER], PhysicalName="[OCTET]", ContainerName="[OCTET]", EntityThresholdType=[INTEGER], EntityThresholdWarning=[INTEGER], EntityThresholdCurrent=[INTEGER], EntityTrapFaultID=[INTEGER])"

The storage usage of the container exceeds the alarm threshold.

NOTE

Only cloud APs support this alarm.

Attribute

Alarm ID	Alarm OID	Alarm Severity	Alarm Type
1707675684	1.3.6.1.4.1.2011.5.25.219.2.42.5	Major	equipmentAlarm

Parameters

Name	Meaning
OID	Indicates the ID of a MIB object.
Index	Indicates the entity index.
HwEntityPhysicalIndex	Indicates the physical entity index.
PhysicalName	Indicates the physical entity name.
ContainerName	Indicates the container name.
EntityThresholdType	Indicates the threshold type.
EntityThresholdWarning	Indicates the alarm threshold.
EntityThresholdCurrent	Indicates the current value.
EntityTrapFaultID	Indicates the error code.

Impact on the System

The container and applications in the container cannot run properly.

Possible Causes

The container or an application in the container is not running properly. As a result, the storage usage of the container exceeds 90%.

Procedure

- Step 1
- Run the **display container information** command to check the status of the container.
- Step 2
- Collect alarm messages, log messages, configurations, and container status information collected in step 1, and contact technical support personnel.
- Step 3
- End.
- End

3.4.204 ALM-1707675685 Abnormal operation of container

Description

ENTITYTRAP/2/CONTAINERABNORMALRISE: "OID [oid] A container fault occurred. (Index=[INTEGER], HwEntityPhysicalIndex=[INTEGER], PhysicalName="[OCTET]", ContainerName="[OCTET]", EntityTrapFaultID=[INTEGER])"

A fault occurs on a container.

Attribute

Alarm ID	Alarm OID	Alarm Severity	Alarm Type
1707675685	1.3.6.1.4.1.2011.5.25.219.2.42.7	Major	equipmentAlarm

Parameters

Name	Meaning
Name	Meaning
OID	Indicates the ID of a MIB object.
Index	Indicates the entity index.
HwEntityPhysicalIndex	Indicates the physical entity index.
PhysicalName	Indicates the physical entity name.
ContainerName	Indicates the container name.
EntityTrapFaultID	Indicates the error code.

Impact on the System

The container and applications in the container cannot run properly.

Possible Causes

A fault occurs on the container or an application in the container.

Procedure

- Step 1

Run the **display container information** command to check the status of the container.
- Step 2

Collect alarm messages, log messages, configurations, and container status information collected in step 1, and contact technical support personnel.
- Step 3

End.
- End

3.4.205 ALM-1707675686 Abnormal operation alarm of APP in container

Description

ENTITYTRAP/2/CONTAINERAPPABNORMALRISE: "OID [oid] An application in the container was faulty.(Index=[INTEGER], HwEntityPhysicalIndex=[INTEGER], PhysicalName="[OCTET]", ContainerName="[OCTET]", AppName="[OCTET]", EntityTrapFaultID=[INTEGER])"

A fault occurs on an application in the container.

Attribute

Alarm ID	Alarm OID	Alarm Severity	Alarm Type
1707675686	1.3.6.1.4.1.2011.5.25.219.2.42.9	Major	equipmentAlarm

Parameters

Name	Meaning
OID	Indicates the ID of a MIB object.
Index	Indicates the entity index.
HwEntityPhysicalIndex	Indicates the physical entity index.
PhysicalName	Indicates the physical entity name.
ContainerName	Indicates the container name.
AppName	Indicates the application name.
EntityTrapFaultID	Indicates the error code.

Impact on the System

The container and applications in the container cannot run properly.

Possible Causes

A fault occurs on the container or an application in the container.

Procedure

- Step 1** Run the **display container information** command to check the status of the container.
- Step 2** Collect alarm messages, log messages, configurations, and container status information collected in step 1, and contact technical support personnel.
- Step 3** End.
- End

3.4.206 ALM-303046418 NETCONF Database Exception

Description

ENTITYTRAP/1/DATABASEEXCEPTION: "OID [oid] The NETCONF database is abnormal."

The NETCONF database is abnormal.



NOTE

Only cloud APs support this alarm.

Attribute

Alarm ID	Alarm OID	Alarm Severity	Alarm Type
303046418	1.3.6.1.4.1.2011.5.2 5.219.2.11.13	Critical	equipmentAlarm

Parameters

Name	Meaning
OID	Indicates the ID of a MIB object.

Impact on the System

When the NETCONF database of the device is abnormal, the device does not respond to the configuration delivered by SDN controlleriMaster NCE-Campus.

Possible Causes

The NETCONF database is abnormal.

Procedure

- Step 1** Restart the device at a proper time and manually clear the alarm.

- If the alarm is cleared, go to step 3.
- If the alarm persists, go to step 2.

Step 2 Collect alarm messages, log messages, and configurations, and then contact technical support personnel.

Step 3 End.

----End

3.4.207 ALM-303046421 The EMDI session on the AP exceeds the threshold

Description

WLAN/4/AP_EMDI_SESSION_OVERLOAD: OID [oid] AP EMDI session number overload notify. (APMAC=[OPAQUE], APName=[STRING], APID=[INTEGER], CurEmdiSessionRate=[INTEGER]%, UpperEmdiSessionThreshold=[INTEGER]%, LowerEmdiSessionThreshold=[INTEGER]%)

The number of eMDI sessions on an AP exceeded the threshold.

Attribute

Alarm ID	Alarm OID	Alarm Severity	Alarm Type
303046421	1.3.6.1.4.1.2011.6.139.13.1.1.143	Warning	Quality of service alarm

Parameters

Name	Meaning
OID	Indicates the ID of a MIB object.
APMAC	Indicates the MAC address of an AP.
APName	Indicates the AP name.
APID	Indicates the AP ID.
CurEmdiSessionRate	Indicates the current eMDI session usage.
UpperEmdiSessionThreshold	Indicates the upper alarm threshold for the eMDI session usage.

Name	Meaning
LowerEmdiSessionThreshold	Indicates the lower alarm threshold for the eMDI session usage.

Impact on the System

New sessions that meet the eMDI analysis criteria on the AP are not added to the session list.

Possible Causes

The number of sessions for eMDI analysis on the AP exceeds 90% of the specifications.

Procedure

- Step 1 Adjust the scope of monitored applications to reduce unimportant applications.
- End

Clearing

After the fault is rectified, the system clears this alarm, removing the need to manually clear it. This alarm will not be displayed on the **CurrentAlarms** page.

3.4.208 ALM-303046422 The SIPFPM flow table on the AP exceeds the threshold

Description

WLAN/4/AP_SIPFPM_FLOW_OVERLOAD: OID [oid] AP s-ipfpm stream number overload. (APMAC=[OPAQUE], APName=[STRING], APID=[INTEGER], CurSipfpmFlowRate=[INTEGER]%, UpperSipfpmFlowThreshold=[INTEGER]%, LoweSipfpmFlowThreshold=[INTEGER]%)

The number of S-IPFPM flows on an AP exceeded the threshold.

Attribute

Alarm ID	Alarm OID	Alarm Severity	Alarm Type
303046422	1.3.6.1.4.1.2011.6.139.13.1.1.145	Warning	Quality of service alarm

Parameters

Name	Meaning
OID	Indicates the ID of a MIB object.
APMAC	Indicates the MAC address of an AP.
APName	Indicates the AP name.
APID	Indicates the AP ID.
CurSipfpmFlowRate	Indicates the current S-IPFPM flow usage.
UpperSipfpmFlowThreshold	Indicates the upper alarm threshold for the S-IPFPM flow usage.
LoweSipfpmFlowThreshold	Indicates the lower alarm threshold for the S-IPFPM flow usage.

Impact on the System

New flows meeting the iPCA analysis criteria on the AP are not added to the flow table.

Possible Causes

The number of flows for iPCA analysis on the AP exceeds 90% of the specifications.

Procedure

- Step 1 Adjust the scope of monitored applications to reduce unimportant applications.
- End

Clearing

After the fault is rectified, the system clears this alarm, removing the need to manually clear it. This alarm will not be displayed on the **CurrentAlarms** page.

3.4.209 ALM-303046423 The number of SIPFPM flow tables on the AP reaches the maximum

Description

WLAN/4/AP_USER_SIPFPM_FLOW_FULL: OID [oid] The s-ipfpm stream number of the terminal reaches the upper limit. (APMAC=[OPAQUE], APName=[STRING], APID=[INTEGER], StaMac=[OPAQUE], MaxUserSipfpmFlowNum=[INTEGER])

The number of S-IPFPM flows of a STA on an AP exceeded the threshold.

Attribute

Alarm ID	Alarm OID	Alarm Severity	Alarm Type
303046423	1.3.6.1.4.1.2011.6.139.18.1.1.1.14	Warning	Quality of service alarm

Parameters

Name	Meaning
OID	Indicates the ID of a MIB object.
APMAC	Indicates the MAC address of an AP.
APName	Indicates the AP name.
APID	Indicates the AP ID.
StaMac	Indicates the MAC address of a STA, which functions as the index for querying its association information.
MaxUserSipfpmFlowNum	Indicates the maximum number of S-IPFPM flows of the STA.

Impact on the System

New flows meeting the iPCA analysis criteria of the STA are not added to the flow table.

Possible Causes

The number of flows for iPCA analysis of the STA exceeds the specifications.

Procedure

- Step 1

Adjust the scope of monitored applications to reduce unimportant applications.
- End

Clearing

After the fault is rectified, the system clears this alarm, removing the need to manually clear it. This alarm will not be displayed on the **CurrentAlarms** page.

3.4.210 ALM-303046424 The SIPFPM flow table on the AC reaches the upper limit

Description

ENTITYTRAP/4/SIPFPM_FLOW_OVERLOAD: OID [oid] The s-ipfpm stream number overload. (Index=[INTEGER], HwEntityPhysicalIndex=[INTEGER], PhysicalName="[OCTET]", CurSipfpmFlowRate=[INTEGER]%, UpperSipfpmFlowThreshold=[INTEGER]%, LoweSipfpmFlowThreshold=[INTEGER]%)

The number of entries in the S-IPFPM flow table reached the upper limit.

Attribute

Alarm ID	Alarm OID	Alarm Severity	Alarm Type
303046424	1.3.6.1.4.1.2011.5.25.219.2.43.1	Warning	Quality of service alarm

Parameters

Name	Meaning
OID	Indicates the ID of a MIB object.
Index	Indicates the entity index.
HwEntityPhysicalIndex	Indicates the physical entity index.
PhysicalName	Indicates the physical entity name.
CurSipfpmFlowRate	Indicates the current S-IPFPM flow usage.
UpperSipfpmFlowThreshold	Indicates the upper alarm threshold for the S-IPFPM flow usage.
LoweSipfpmFlowThreshold	Indicates the lower alarm threshold for the S-IPFPM flow usage.

Impact on the System

New flows meeting the iPCA analysis criteria are not added to the flow table.

Possible Causes

The number of flows for iPCA analysis exceeds 90% of the specifications.

Procedure

Step 1 Adjust the scope of monitored flows to reduce unimportant flows.

----End

Clearing

After the fault is rectified, the system clears this alarm, removing the need to manually clear it. This alarm will not be displayed on the **CurrentAlarms** page.

3.4.211 ALM-3276800750 The CA certificate is nearly expired.

Description

PKI/4/PKICACERTNEARLYEXPIRED: OID [oid] the CA certificate is nearly expired. (APMAC=[OPAQUE], APName=[STRING], APID=[INTEGER], CACertIssuer=[issuer], CACertSubject=[subject], CACertStartTime=[starttime], CACertFinishTime=[finishtime])

The CA certificate is about to expire.

Attribute

AlarmID	Alarm Severity	Alarm Type
3276800750	Warning	Quality of service alarm

Parameters

Name	Meaning
oid	Indicates the MIB object ID of the alarm.
APMAC	MAC address of an AP.
APName	AP name.
APID	AP ID.
CACertIssuer	Indicates the issuer of the CA certificate.
CACertSubject	Indicates the subject of the CA certificate.
CACertStartTime	Indicates the start time of the CA certificate.
CACertFinishTime	Indicates the end time of the CA certificate.

Impact on the System

The service will be invalid after the certificate expires.

Possible Causes

The CA certificate is about to expire. The CA certificate expiration time is less than the certificate expired prewarning time configured by the **pki set-certificate expire-prewarning** command.

Procedure

1. Run the **display clock** command to check whether the device time is correct.
If not, run the **clock datetime** command in the user view to change the device time.
2. Apply for a new certificate through SCEP or CMPv2 online or apply for a new certificate offline.

3.4.212 ALM-3276801006 The local certificate is nearly expired

Description

PKI/4/PKILOCALCERTVALID: OID [*oid*] the local certificate is valid.
(LocalCertIssuer=[*issuer*], LocalCertSubject=[*subject*],
LocalCertStartTime=[*starttime*], LocalCertFinishTime=[*finishtime*])

The local certificate is valid.

Attribute

AlarmID	Alarm Severity	Alarm Type
3276801006	Warning	Quality of service alarm

Parameters

Name	Meaning
oid	Indicates the MIB object ID of the alarm.
APMAC	MAC address of an AP.
APName	AP name.
APID	AP ID.
LocalCertIssuer	Indicates the issuer of the local certificate.

Name	Meaning
LocalCertSubject	Indicates the subject of the local certificate.
LocalCertStartTime	Indicates the start time of the local certificate.
LocalCertFinishTime	Indicates the end time of the local certificate.

Impact on the System

The service will be invalid after the certificate expires.

Possible Causes

The local certificate is about to expire. The local certificate expiration time is less than the certificate expired prewarning time configured by the **pki set-certificate expire-prewarning** command.

Procedure

1. Check whether the system time on the local device is correct.
2. If the system time is correct, apply for a new local certificate immediately.

3.4.213 ALM-4286849026 The CPE device generate an alarm

Description

WLAN/4/CPE_REPORT_ALARM: OID [oid] The CPE device generate an alarm.
(CPEMac=[OPAQUE], APMac=[OPAQUE], APName=[STRING], APID=[INTEGER], AlarmContent=[STRING])

An AP reports alarm information about a CPE.

Attribute

AlarmID	Alarm Severity	Alarm Type
4286849026	Warning	Quality of service alarm

Parameters

Name	Meaning
OID	Indicates the ID of a MIB object.
CPEMac	Indicates the MAC address of a CPE.

Name	Meaning
APMac	Indicates the MAC address of an AP.
APName	Indicates the AP name.
APID	Indicates the AP ID.
AlarmContent	Indicates the alarm content reported by the CPE.

Impact on the System

None.

Possible Causes

In a CPE management scenario, upon an exception on a CPE, the AP reports alarm information about the CPE, requiring cause analysis.

Procedure

Contact the vendor of the CPE to analyze the alarm cause and provide suggestions for clearing the alarm.

3.5 V600 Device Alarms

3.5.1 Common Alarms

3.5.1.1 ALM-15795031 CPU_BUSY

Description

The CPU usage exceeded the pre-set overload threshold.
(TrapSeverity=[TrapSeverity], ProbableCause=[ProbableCause],
EventType=[EventType], PhysicalIndex=[PhysicalIndex],
PhysicalName=[PhysicalName], RelativeResource=[RelativeResource],
UsageType=[UsageType], SubIndex=[SubIndex], CpuUsage=[CpuUsage],
Unit=[Unit], CpuUsageThreshold=[CpuUsageThreshold]).

The CPU usage is continuously sampled. This alarm is generated when the CPU usage sampled each time is greater than the overload threshold in a sampling period (Number of continuous CPU overload times x Sampling interval).

Attribute

Alarm ID	OID	Alarm Severity	Alarm Type
15795031	1.3.6.1.4.1.2011.5.25.129.2.4.1	Critical	Quality of service alarm

Parameters

Name	Meaning
TrapSeverity	Indicates the alarm severity.
ProbableCause	Alarm cause.
EventType	Indicates the alarm type.
PhysicalIndex	Physical index.
PhysicalName	Entity name.
RelativeResource	Relevant resource name.
UsageType	Overload type.
SubIndex	Entity sub-index.
CpuUsage	CPU usage.
Unit	Indicates the unit.
CpuUsageThreshold	Overload threshold.

Impact on the System

- Cause 74299: The CPU usage exceeded the pre-set overload threshold.
If the CPU usage is high for a long period of time, services cannot be processed in time, and the system performance is affected.
The system performance, for example, time taken to process user operations, neighbor status, and route convergence performance, will be affected.
- Cause 74300: CPU usage of the data plane includes the CPU usage of basic forwarding services and other data plane services.
The usage of a single forwarding CPU exceeds the alarm threshold. If the forwarding traffic exceeds the forwarding performance of the device, service forwarding is affected and packet loss occurs.

Possible Causes

- Cause 74299: The CPU usage exceeded the pre-set overload threshold.
- Cause 74300: CPU usage of the data plane includes the CPU usage of basic forwarding services and other data plane services.

Procedure

- Cause 74299: The CPU usage exceeded the pre-set overload threshold.
 - a. Run the `display cpu-usage` command to check the CPU usage and its overload threshold.
 - If CPU usage exceeds the overload threshold, go to Step 2.
 - If CPU usage is below the overload threshold, go to Step 4.
 - b. Delete unnecessary services and configurations to reduce CPU usage, and then check whether the alarm is cleared.
 - If the clear alarm is generated, the fault is rectified.
 - If this alarm persists, go to Step 3.
 - c. Run the `set cpu-usage threshold` command to adjust the overload threshold, and then check whether the alarm is cleared.
 - If the clear alarm is generated, the fault is rectified.
 - If this alarm persists, go to Step 4.
 - d. Collect the alarm information, log information, and configuration information, and contact Huawei technical support engineers.
- Cause 74300: CPU usage of the data plane includes the CPU usage of basic forwarding services and other data plane services.

Check the service usage in the `display cpu-usage` command output and perform capacity expansion based on service requirements.

Clearing

After the fault is rectified, the system clears this alarm, removing the need to manually clear it. This alarm will not be displayed on the **CurrentAlarms** page.

3.5.1.2 ALM-135462939 hwPowerInvalid

Description

A power module experienced a complete failure.
(EntPhysicalIndex=[EntPhysicalIndex], EntPhysicalName=[EntPhysicalName], EntityTrapFaultID=[EntityTrapFaultID], EntityOperStatus=[EntityOperStatus], Reason=[ReasonDsp])

The power module completely failed.

Attribute

Alarm ID	OID	Alarm Severity	Alarm Type
135462939	1.3.6.1.4.1.2011.5.25.219.2.5.5	Major	Equipment alarm

Parameters

Name	Meaning
EntPhysicalIndex	Indicates the index of an entity.
EntPhysicalName	Indicates the name of an entity.
EntityTrapFaultID	Indicates the error code.
EntityOperStatus	Indicates the Status.
ReasonDsp	Indicates a possible cause.

Impact on the System

- Cause 1: Over-input-voltage occurred on the power module.
The system does not support 110 V input.
- Cause 2: Under-input-voltage occurred on the power module.
The system does not support 110 V input.
- Cause 3: The power module supply failed.
The system does not support 110 V input.
- Cause 4: Over-temperature occurred on the power module.
The system does not support 110 V input.
- Cause 5: The power module was installed but not powered on.
The system does not support 110 V input.
- Cause 6: The output of the power module failed.
The system does not support 110 V input.
- Cause 7: Over-output-voltage occurred on the power module.
The system does not support 110 V input.
- Cause 8: The power was not present.
The system does not support 110 V input.
- Cause 9: The actual power exceeded the rated power.
The system does not support 110 V input.
- Cause 10: The power module is in overtemperature protection state.
The system does not support 110 V input.

- Cause 11: The power backplane cable was not installed properly.
Communication with the power module fails, and the power module cannot be controlled by the system.
- Cause 12: The input AC voltage is too low.
The system does not support 110 V input.
- Cause 13: The power type does not match the type of the backplane.
If the power supply is faulty, the power supply to the device may be insufficient. As a result, the board may be reset due to insufficient power supply, which indirectly affects services and needs to be handled.
- Cause 14: The A plane power supply on the power module is faulty.
This failure will result in insufficient power supply on the device, thus powering off or resetting a board and indirect impacting services. Thus, a speedy solution is required.
- Cause 15: The B plane power supply on the power module is faulty.
This failure will result in insufficient power supply on the device, thus powering off or resetting a board and indirect impacting services. Thus, a speedy solution is required.
- Cause 16: The A plane power supply on the power module is over voltage.
If the power supply is faulty, the power supply to the device may be insufficient. As a result, the board may be reset due to insufficient power supply, which indirectly affects services and needs to be handled.
- Cause 17: The B plane power supply on the power module is over voltage.
If the power supply is faulty, the power supply to the device may be insufficient. As a result, the board may be reset due to insufficient power supply, which indirectly affects services and needs to be handled.
- Cause 18: The A plane power supply on the power module is under voltage.
If the power supply is faulty, the power supply to the device may be insufficient. As a result, the board may be reset due to insufficient power supply, which indirectly affects services and needs to be handled.
- Cause 19: The B plane power supply on the power module is under voltage.
If the power supply is faulty, the power supply to the device may be insufficient. As a result, the board may be reset due to insufficient power supply, which indirectly affects services and needs to be handled.
- Cause 20: Under-output-voltage occurred on the power module.
The power supply of the power module is abnormal. As a result, the board may be reset due to insufficient power supply, which indirectly affects services and needs to be handled.

Possible Causes

- Cause 1: Over-input-voltage occurred on the power module
- Cause 2: Under-input-voltage occurred on the power module.
- Cause 3: The power module supply failed.
- Cause 4: Over-temperature occurred on the power module.
- Cause 5: The power module was installed but not powered on.

- Cause 6: The output of the power module failed.
- Cause 7: Over-output-voltage occurred on the power module.
- Cause 8: The power was not present.
- Cause 9: The actual power exceeded the rated power.
- Cause 10: The power module is in overtemperature protection state.
- Cause 11: The power backplane cable was not installed properly.
- Cause 12: The input AC voltage is too low.
- Cause 13: The power type does not match the type of the backplane.
- Cause 14: The A plane power supply on the power module is faulty.
- Cause 15: The B plane power supply on the power module is faulty.
- Cause 16: The A plane power supply on the power module is over voltage.
- Cause 17: The B plane power supply on the power module is over voltage.
- Cause 18: The A plane power supply on the power module is under voltage.
- Cause 19: The B plane power supply on the power module is under voltage.
- Cause 20: Under-output-voltage occurred on the power module.

Procedure

- Cause 1: Over-input-voltage occurred on the power module.
 - a. Check whether the external power supply is proper. If not, repair the external circuit.
 - b. If the fault persists, replace the power module.
- Cause 2: Under-input-voltage occurred on the power module.
 - a. Check whether the external power supply is proper. If not, repair the external circuit.
 - b. If the fault persists, replace the power module.
- Cause 3: The power module supply failed.
 - a. Check whether the fan of the power module cannot work because the air filter is clogged. If so, clean the air filter.
 - b. Check whether the ambient temperature is within the allowed range. If the temperature is too high, improve heat dissipation.
 - c. Check whether the power supply is normal. If not, repair the external power supply circuit.
 - d. If the fault persists, replace the power module.
- Cause 4: Over-temperature occurred on the power module.
 - 1. Check whether the fan of the power module cannot work because the air filter is clogged. If so, clean the air filter.
 - 2. Check whether the ambient temperature is within the allowed range. If the temperature is too high, improve heat dissipation.
 - 3. Check whether the power supply is normal. If not, repair the external power supply circuit.
 - 4. If the fault persists, replace the power module.
- Cause 5: The power module was installed but not powered on.

- a. Power on the power module.
- Cause 6: The output of the power module failed.
 - a. Check whether the external power supply is proper. If not, repair the external circuit.
 - b. If the fault persists, replace the power module.
- Cause 7: Over-output-voltage occurred on the power module.
 - a. Check whether the external power supply is proper. If not, repair the external circuit.
 - b. If the fault persists, replace the power module.
- Cause 8: The power was not present.
 - a. Check whether the power module is properly installed. If not, remove and then reinstall the power module properly.
- Cause 9: The actual power exceeded the rated power.
 - a. Check whether the power module is a standard power module. If not, replace the power module. If the power module is a standard one, contact technical support personnel.
- Cause 10: The power module is in overtemperature protection state.
 - a. The handling procedure is the same as that for cause 5.
- Cause 11: The power backplane cable was not installed properly.
 - a. Remove and then install the power module.
 - b. Collect traps, logs, and configurations, and contact technical support personnel.
- Cause 12: The input AC voltage is too low.
 - a. Connect the device to a power supply system whose voltage is greater than 165 V.
 - b. Check the product manual to determine the supported power module types.
- Cause 13: The power type does not match the type of the backplane.
 - a. Check whether the power module and backplane types match. If they do not match, replace the power module with one matching the backplane type and then check whether the trap is cleared.
 - If the trap is cleared, go to Step 3.
 - If the trap persists, go to Step 2.
 - b. Collect trap, log, and configuration information, and contact technical support personnel.
 - c. End.
- Cause 14: The A plane power supply on the power module is faulty.
 - a. Check whether the external power supply is normal.
 - If not, go to step 2.
 - If so, go to step 3.

- b. Repair the external power supply circuit.
 - If so, go to step 5.
 - If not, go to step 3.
 - c. Replace the power module.
 - If so, go to step 5.
 - If not, go to step 4.
 - d. Collect trap, log, and configuration information, and contact technical support personnel.
 - e. End.
- Cause 15: The B plane power supply on the power module is faulty.
 - a. Check whether the external power supply is normal.
 - If not, go to step 2.
 - If so, go to step 3.
 - b. Repair the external power supply circuit.
 - If so, go to step 5.
 - If not, go to step 3.
 - c. Replace the power module.
 - If so, go to step 5.
 - If not, go to step 4.
 - d. Collect trap, log, and configuration information, and contact technical support personnel.
 - e. End.
- Cause 16: The A plane power supply on the power module is over voltage.
 - a. Check whether the external power supply is normal.
 - If not, go to step 2.
 - If so, go to step 3.
 - b. Repair the external power supply circuit.
 - If so, go to step 5.
 - If not, go to step 3.
 - c. Replace the power module.
 - If so, go to step 5.
 - If not, go to step 4.
 - d. Collect trap, log, and configuration information, and contact technical support personnel.

- e. End.
- Cause 17: The B plane power supply on the power module is over voltage.
 - a. Check whether the external power supply is normal.
 - If not, go to step 2.
 - If so, go to step 3.
 - b. Repair the external power supply circuit.
 - If so, go to step 5.
 - If not, go to step 3.
 - c. Replace the power module.
 - If so, go to step 5.
 - If not, go to step 4.
 - d. Collect trap, log, and configuration information, and contact technical support personnel.
 - e. End.
- Cause 18: The A plane power supply on the power module is under voltage.
 - a. Check whether the external power supply is normal.
 - If not, go to step 2.
 - If so, go to step 3.
 - b. Repair the external power supply circuit.
 - If so, go to step 5.
 - If not, go to step 3.
 - c. Replace the power module.
 - If so, go to step 5.
 - If not, go to step 4.
 - d. Collect trap, log, and configuration information, and contact technical support personnel.
 - e. End.
- Cause 19: The B plane power supply on the power module is under voltage
 - a. Check whether the external power supply is normal.
 - If not, go to step 2.
 - If so, go to step 3.
 - b. Repair the external power supply circuit.
 - If so, go to step 5.
 - If not, go to step 3.

- c. Replace the power module.
 - If so, go to step 5.
 - If not, go to step 4.
- d. Collect trap, log, and configuration information, and contact technical support personnel.
- e. End.
- Cause 20: Under-output-voltage occurred on the power module.
 - a. Check whether the external power supply is normal. If the external power supply is abnormal, repair the external circuit.
 - b. If the alarm persists, replace the power module.

Clearing

After the fault is rectified, the system clears this alarm, removing the need to manually clear it. This alarm will not be displayed on the **Current Alarms** page.

3.5.1.3 ALM-15795032 hwStorageUtilizationRisingAlarm

Description

The storage usage exceeded the pre-set overload threshold.
(TrapSeverity=[TrapSeverity], ProbableCause=[ProbableCause], EventType=[EventType], PhysicalIndex=[PhysicalIndex], PhysicalName=[PhysicalName], RelativeResource=[RelativeResource], UsageType=[UsageType], SubIndex=[SubIndex], UsageValue=[UsageValue], Unit=[Unit], UsageThreshold=[UsageThreshold])

Memory or storage usage was sampled for a period of time. In one sampling period (overload times x sampling interval), if each memory or storage usage sample exceeded the pre-set overload threshold, this alarm was generated.

Attribute

Alarm ID	OID	Alarm Severity	Alarm Type
15795032	1.3.6.1.4.1.2011.5.25.129.2.6.1	Major	Quality of service alarm

Parameters

Name	Meaning
TrapSeverity	Alarm severity.

Name	Meaning
ProbableCause	Possible cause, values are as follows: • 75264: Memory usage exceeded the overload threshold. • 75265: Storage usage exceeded the overload threshold.
EventType	Alarm type.
PhysicalIndex	Physical index.
PhysicalName	Entity name.
RelativeResource	Relevant resource name.
UsageType	Overload type.1 indicates the CPU, 2 indicates the memory, 3 indicates the disk, 4 indicates the flash memory, 5 indicates the CF card, and 6 indicates the physical memory.
SubIndex	Entity sub-index.
UsageValue	Storage usage.
Unit	Unit.
UsageThreshold	Overload threshold.

Impact on the System

- Cause 75264: The memory usage exceeded the pre-set overload threshold.
If services cannot successfully obtain memory resources, the system automatically restarts.
- Cause 75265: The storage usage exceeded the pre-set overload threshold.
If the remaining space in the storage medium is insufficient, the log function and software upgrade are affected.

Possible Causes

- Cause 75264: The memory usage exceeded the pre-set overload threshold.
- Cause 75265: The storage usage exceeded the pre-set overload threshold.

Procedure

- Cause 75264: The memory usage exceeded the pre-set overload threshold.

- a. Run the **display system memory statistics** command to view the memory usage, and run the **display memory threshold** command to view the overload threshold.
 - If the memory usage exceeded the overload threshold, go to Step 2.
 - If the memory usage is below the overload threshold, go to Step 4.
 - b. Reduce unnecessary services or delete unnecessary configurations to reduce the memory usage, and then check whether this alarm is cleared. When deleting service configurations, submit 3~5 configurations at a time.
 - If this alarm is cleared, it indicates that the problem is solved.
 - If this alarm persists, go to Step 3.
 - c. Run the **set memory threshold** command to change the overload threshold, and then check whether this alarm is cleared.
 - If this alarm is cleared, it indicates that the problem is solved.
 - If this alarm persists, go to Step 4.
4. Collect the alarm information, log information, and configuration information, and contact Huawei technical support engineers.
- Cause 75265: The storage usage exceeded the pre-set overload threshold.
 - a. Run the **cd** command to access the directory, and run the **dir** command to view the storage usage.
 - If the storage usage exceeded the overload threshold, go to Step 2.
 - If the storage usage is below the overload threshold, go to Step 3.
 - b. Delete unnecessary files to reduce the storage usage.
 - If this alarm is cleared, it indicates that the problem is solved.
 - If this alarm persists, go to Step 3.
 - c. Collect the alarm information, log information, and configuration information, and contact technical support engineers.

Clearing

After the fault is rectified, the system clears this alarm, removing the need to manually clear it. This alarm will not be displayed on the **Current Alarms** page.

3.5.1.4 ALM-135462943 hwPowerRemove

Description

The power module was removed. (EntPhysicalIndex=[EntPhysicalIndex], EntPhysicalName=[EntPhysicalName], EntityTrapFaultID=[EntityTrapFaultID], EntityOperStatus=[EntityOperStatus], Reason=[ReasonDsp])

A power module was removed.

Attribute

Alarm ID	OID	Alarm Severity	Alarm Type
135462943	1.3.6.1.4.1.2011.5.25.219.2.5.1	Critical	Equipment alarm

Parameters

Name	Meaning
EntPhysicalIndex	Indicates the index of an entity.
EntPhysicalName	Indicates the name of an entity.
EntityTrapFaultID	Indicates the error code.
EntityOperStatus	Indicates the Status.
ReasonDsp	Indicates a possible cause.

Impact on the System

The power module is removed, which may cause insufficient power supply. If the power supply is insufficient, the board may be powered off. This affects services. This fault needs to be rectified.

Possible Causes

A power module was removed.

Procedure

1. Check whether the power module is installed.
2. If so, check whether the power module is installed correctly.
3. If the power module is installed correctly but the fault persists, replace the power module.
4. If the fault persists after the power module is replaced, collect traps, logs, and configurations, and contact technical support personnel.

Clearing

After the fault is rectified, the system clears this alarm, removing the need to manually clear it. This alarm will not be displayed on the **Current Alarms** page.

3.5.1.5 ALM-135462937 hwFanRemove

Description

The fan module was removed. (EntPhysicalIndex=[EntPhysicalIndex], EntPhysicalName=[EntPhysicalName], EntityTrapFaultID=[EntityTrapFaultID], EntityOperStatus=[EntityOperStatus], Reason=[ReasonDsp])

A fan was removed.

Attribute

Alarm ID	OID	Alarm Severity	Alarm Type
135462937	1.3.6.1.4.1.2011.5.25.219.2.6.1	Major	Equipment alarm

Parameters

Name	Meaning
EntPhysicalIndex	Indicates the entity index.
EntPhysicalName	Indicates the name of an entity.
EntityTrapFaultID	Indicates the error code.
EntityOperStatus	Indicates the Status.
ReasonDsp	Indicates a possible cause.

Impact on the System

A fault of the fan module affects heat dissipation performance of the device and increases the temperature of the device. Services are not affected in a short time, but the fault should be rectified quickly.

Possible Causes

A fan module was removed.

Procedure

- Check whether the fan is installed.
 - If so, go to step 2.
 - If not, install the fan correctly.
 - Check whether the fan is installed properly.

- If so, replace the fan.
- If not, install the fan correctly.

Clearing

After the fault is rectified, the system clears this alarm, removing the need to manually clear it. This alarm will not be displayed on the **CurrentAlarms** page.

3.5.1.6 ALM-135462925 hwBrdTempAlarm

Description

The board temperature exceeded the upper alarm threshold.
(EntPhysicalIndex=[EntPhysicalIndex], EntPhysicalName=[EntPhysicalName], EntityThresholdType=[EntityThresholdType], EntityThresholdWarning=[EntityThresholdWarning], EntityThresholdCurrent=[EntityThresholdCurrent], EntityTrapFaultID=[EntityTrapFaultID], Reason=[ReasonDsp])

The board or card temperature was too high.

Attribute

Alarm ID	OID	Alarm Severity	Alarm Type
135462925	1.3.6.1.4.1.2011.5.25.219.2.10.13	Minor	Environmental alarm

Parameters

Name	Meaning
EntPhysicalIndex	Indicates the index of an entity.
EntPhysicalName	Indicates the name of an entity.
EntityThresholdType	Indicates the threshold type of the entity.
EntityThresholdWarning	Indicates the temperature threshold of the entity.
EntityThresholdCurrent	Indicates the current temperature.
EntityTrapFaultID	Indicates the error code.
ReasonDsp	Indicates a possible cause.

Impact on the System

- Cause 1: Services are not affected temporarily, but the subcard temperature needs to be lowered as soon as possible.
- Cause 2: Services are not affected temporarily, but the board temperature needs to be lowered as soon as possible.
- Cause 3: Services are not affected temporarily, but the board temperature needs to be increased as soon as possible.
- Cause 4: Services are not affected temporarily, but the subcard temperature needs to be increased as soon as possible.

Possible Causes

- Cause 1: The card temperature was too high.
- Cause 2: The board temperature was too high.
- Cause 3: The board temperature fell below the lower limit.
- Cause 4: The subcard temperature fell below the lower limit.

Procedure

- Cause 1: The card temperature was too high.
 - a. Check whether the air filter of the fan is blocked.
 - If so, clean the air filter.
 - If not, go to step 2.
 - b. Check whether the ambient temperature is too high.
 - If so, reduce the ambient temperature.
 - If not, go to step 3.
 - c. Check whether the fan is faulty.
 - If so, rectify the fan fault.
 - If not, go to step 4.
 - d. Check whether a filler panel is installed in the slot that has no subcard installed.
 - If so, go to step 5.
 - If not, install a filler panel in the slot.
 - e. Collect traps, logs, and configurations, and contact technical support personnel.
- Cause 2: The board temperature was too high.
 - a. Check whether the air filter of the fan is blocked.
 - If so, clean the air filter.
 - If not, go to step 2.
 - b. Check whether the ambient temperature is too high.

- If so, reduce the ambient temperature.
- If not, go to step 3.
- c. Check whether the fan is faulty.
 - If so, rectify the fan fault.
 - If not, go to step 4.
- d. Check whether a filler panel is installed in the slot that has no board installed.
 - If so, go to step 5.
 - If not, install a filler panel in the slot.
- e. Collect traps, logs, and configurations, and contact technical support personnel.
- Cause 3: The board temperature fell below the lower limit.
 - a. Adjust the ambient temperature or increase the distance between the device and the air conditioner.
 - b. Collect trap, log, and configuration information, and contact Huawei technical support personnel.
- Cause 4: The subcard temperature fell below the lower limit.
 - a. Adjust the ambient temperature or increase the distance between the device and the air conditioner. Collect trap, log, and configuration information, and contact Huawei technical support personnel.

Clearing

After the fault is rectified, the system clears this alarm, removing the need to manually clear it. This alarm will not be displayed on the **Current Alarms** page.

3.5.1.7 ALM-139591683 linkDown

Description

The interface status changes. (ifName=[ifName], AdminStatus=[ifAdminStatus], OperStatus=[ifOperStatus], Reason=[Reason], mainIfname=[mainIf])

The interface status changes.

Attribute

Alarm ID	OID	Alarm Severity	Alarm Type
139591683	1.3.6.1.6.3.1.1.5.3	Major	Equipment alarm

Parameters

Name	Meaning
ifName	Interface name
ifAdminStatus	Interface admin status.
ifOperStatus	Current interface status
Reason	Reason for trap generation
mainIf	Name of the main interface

Impact on the System

The interface cannot forward packets normally.

Possible Causes

- Cause 1: Interface physical link is down.
- Cause 2: LACP negotiation failed.
- Cause 3: Receive ConfReq packet.
- Cause 4: Receive ConfAck packet.
- Cause 5: Receive Nak packet.
- Cause 6: Receive Term packet.
- Cause 7: Receive TermAck packet.
- Cause 8: Receive CodeRej packet.
- Cause 9: Receive ProtoRej packet.
- Cause 10: CHAP authentication failed.
- Cause 11: PAP authentication failed.
- Cause 12: Keepalive timer expires.
- Cause 13: The PVC is Down.
- Cause 14: EFM DOWN.
- Cause 15: The tunnel is down.
- Cause 16: The interface is shut down.
- Cause 17: The link protocol is down.
- Cause 19: The link protocol is up.
- Cause 20: The main interface is down.
- Cause 21: Interface physical link is up.
- Cause 22: The conditions for the activation of the interface are not met.
- Cause 23: The conditions for the activation of the interface are met
- Cause 24: The tunnel is up.

- Cause 25: The interface is deleted.
- Cause 26: BFD session is down.
- Cause 27: BFD session is up.
- Cause 28: EFM UP
- Cause 30: DLDP detect down.
- Cause 31: DLDP detect up.
- Cause 32: VRRP FLOW DOWN.
- Cause 33: VRRP FLOW UP.
- Cause 34: VE FLOW DOWN.
- Cause 35: VE FLOW UP.
- Cause 36: The interface is error down.
- Cause 37: CRC ERR DOWN.
- Cause 38: CRC ERR UP
- Cause 39: Transceiver speed does not match the speed configured on the port.
- Cause 40: The port does not support current transceiver.
- Cause 41: Transceiver does not support the negotiation configuration on the port.
- Cause 43: The interface is trigger down.
- Cause 48: CFM DOWN.
- Cause 49: CFM UP.
- Cause 51: The sub-interface linkDown alarm is disabled.

Procedure

- Cause 1: Interface physical link is down.
 - a. Run the **display this** command in the interface view to check whether the interfaces at both ends are shut down. If the interfaces are sub-interfaces, check whether VLAN IDs are configured for the interfaces at both ends.
 - If the interface is a sub-interface, run the **vlan-type dot1q** command to configure a correct VLAN ID for the sub-interface. Then, check whether the alarm is cleared. If the alarm persists, go to Step 2.
 - If the interface is not shut down, go to Step 2.
 - b. Check whether the physical link is normal, for example, whether the network cable or optical module is loose or disconnected.
 - If the physical link is abnormal, reconnect the physical link and check whether the alarm is cleared. If the alarm persists, go to Step 3.
 - If the physical link works properly, go to Step 3.
 - c. Collect alarm and configuration information, and contact technical support personnel.
- Cause 2: LACP negotiation failed.
 - a. Run the **display interface** command in the system view to check whether the local or remote interface is Down.

- If either interface is Down, run the **undo shutdown** command in the interface view, and then check whether the alarm is cleared. If the alarm is not cleared, go to Step 2.
- If the interface status is Up, go to Step 2.
- b. Run the **display interface eth-trunk** command in the system view to check whether the number of local and remote interfaces that are added to an Eth-Trunk is greater than the upper threshold for the number of member links.
 - If the number of local and remote interfaces that are added to the Eth-Trunk is greater than the upper threshold for the number of member links, run the **max active-linknumber** command in the Eth-Trunk interface view to configure a proper upper threshold for the number of member links, and then check whether the alarm is cleared. If the alarm is not cleared, go to Step 4.
 - If the number of local and remote interfaces that are added to the Eth-Trunk is smaller than the upper threshold for the number of member links, go to Step 3.
- c. Run the **display interface eth-trunk** command in the system view to check whether the number of local and remote interfaces that are added to an Eth-Trunk is smaller than the lower threshold for the number of member links.
 - If the number of local and remote interfaces that are added to the Eth-Trunk is smaller than the lower threshold for the number of member links, run the **least active-linknumber** command in the Eth-Trunk interface view to configure a proper lower threshold for the number of member links, and then check whether the alarm is cleared. If the alarm is not cleared, go to Step 4.
 - If the number of local and remote interfaces that are added to the Eth-Trunk is smaller than the lower threshold for the number of member links is greater than the lower threshold of member links on the Eth-Trunk interface, go to Step 4.
- d. Collect alarm information and configuration information, and then contact technical support personnel.
- Cause 3: Receive ConfReq packet.
 - a. Run the **display interface** command in the system view to check whether the PPP protocol of the remote device works properly.
 - If the PPP protocol of the remote device works properly, run the **display interface** command to check the physical link statuses of the devices (including the intermediate device), such as the number of lost packets and error packets. If the physical link statuses are normal but the alarm is not cleared, go to Step 2.
 - If the PPP protocol of the remote device works improperly, contact the engineer responsible for the remote device to rectify the fault. If the fault is rectified but the alarm is not cleared, go to Step 2.
 - b. Collect alarm information and configuration information, and then contact technical support personnel.

- Cause 4: Receive ConfAck packet.
 - a. Run the **display interface** command in the system view to check whether the PPP protocol of the remote device is works properly.
 - If the PPP protocol of the remote device works properly, run the **display interface** command to check the physical link statuses of the devices (including the intermediate device), such as the number of lost packets and error packets. If the physical link statuses are normal but the alarm is not cleared, go to Step 2.
 - If the PPP protocol of the remote device works improperly, contact the engineer responsible for the remote device to rectify the fault. If the fault is rectified but the alarm is not cleared, go to Step 2.
 - 2. Collect alarm information and configuration information, and then contact technical support personnel.
- Cause 5: Receive Nak packet.
 - a. Run the **display interface** command in the system view to check whether the PPP protocol of the remote device is works properly.
 - If the PPP protocol of the remote device works properly, run the **display interface** command to check the physical link statuses of the devices (including the intermediate device), such as the number of lost packets and error packets. If the physical link statuses are normal but the alarm is not cleared, go to Step 2.
 - If the PPP protocol of the remote device works improperly, contact the engineer responsible for the remote device to rectify the fault. If the fault is rectified but the alarm is not cleared, go to Step 2.
 - b. Collect alarm information and configuration information, and then contact technical support personnel.
- Cause 6: Receive Term packet.
 - a. Run the **display interface** command in the system view to check whether the PPP protocol of the remote device is works properly.
 - If the PPP protocol of the remote device works properly, run the **display interface** command to check the physical link statuses of the devices (including the intermediate device), such as the number of lost packets and error packets. If the physical link statuses are normal but the alarm is not cleared, go to Step 2.
 - If the PPP protocol of the remote device works improperly, contact the engineer responsible for the remote device to rectify the fault. If the fault is rectified but the alarm is not cleared, go to Step 2.
 - b. Collect alarm information and configuration information, and then contact technical support personnel.
- Cause 7: Receive TermAck packet.
 - a. Run the **display interface** command in the system view to check whether the PPP protocol of the remote device is works properly.
 - If the PPP protocol of the remote device works properly, run the **display interface** command to check the physical link statuses of the devices (including the intermediate device), such as the number of

lost packets and error packets. If the physical link statuses are normal but the alarm is not cleared, go to Step 2.

- If the PPP protocol of the remote device works improperly, contact the engineer responsible for the remote device to rectify the fault. If the fault is rectified but the alarm is not cleared, go to Step 2.
- b. Collect alarm information and configuration information, and then contact technical support personnel.
- Cause 8: Receive CodeRej packet.
 - a. Run the **display interface** command in the system view to check whether the PPP protocol of the remote device is works properly.
 - If the PPP protocol of the remote device works properly, run the **display interface** command to check the physical link statuses of the devices (including the intermediate device), such as the number of lost packets and error packets. If the physical link statuses are normal but the alarm is not cleared, go to Step 2.
 - If the PPP protocol of the remote device works improperly, contact the engineer responsible for the remote device to rectify the fault. If the fault is rectified but the alarm is not cleared, go to Step 2.
 - b. Collect alarm information and configuration information, and then contact technical support personnel.
- Cause 9: Receive ProtoRej packet.
 - a. Run the **display interface** command in the system view to check whether the PPP protocol of the remote device is works properly.
 - If the PPP protocol of the remote device works properly, run the **display interface** command to check the physical link statuses of the devices (including the intermediate device), such as the number of lost packets and error packets. If the physical link statuses are normal but the alarm is not cleared, go to Step 2.
 - If the PPP protocol of the remote device works improperly, contact the engineer responsible for the remote device to rectify the fault. If the fault is rectified but the alarm is not cleared, go to Step 2.
 - b. Collect alarm information and configuration information, and then contact technical support personnel.
- Cause 10: CHAP authentication failed.
 - a. Run the **display this** command in the interface view to check whether the local end is a server end (authenticating end) or a client end (authenticated end).
 - If the local end is the server end, check whether the user and password configured on the remote end are correct. If they are incorrect, run the local-user password command in the AAA view to re-configure them. Then, check whether the alarm is cleared. If the alarm is not cleared, go to Step 2.
 - If the local end is the client end, run the **display this** command to check whether the user and password configured on the local end are correct. If they are incorrect, run the local-user password

- command in the AAA view to re-configure them. Then, check whether the alarm is cleared. If the alarm is not cleared, go to Step 2.
- b. Collect alarm information and configuration information, and then contact technical support personnel.
- Cause 11: PAP authentication failed.
 - a. Run the **display this** command in the interface view to check whether the local end is a server end (authenticating end) or a client end (authenticated end).
 - If the local end is the server end, check whether the user and password configured on the remote end are correct. If they are incorrect, run the **local-user password** command in the AAA view to re-configure them. Then, check whether the alarm is cleared. If the alarm is not cleared, go to Step 2.
 - If the local end is the client end, run the **display this** command to check whether the user and password configured on the local end are correct. If they are incorrect, run the **local-user password** command in the AAA view to re-configure them. Then, check whether the alarm is cleared. If the alarm is not cleared, go to Step 2.
 - 2. Collect alarm information and configuration information, and then contact technical support personnel.
 - Cause 12: Keepalive timer expires.
 - a. Run the **display interface** command in the system view to check whether the PPP protocol of the remote device works properly.
 - If the PPP protocol of the remote device works properly, run the **display interface** command to check the physical link statuses of the devices (including the intermediate device), such as the number of lost packets and error packets. If the physical link statuses are normal but the alarm is not cleared, go to Step 2.
 - If the PPP protocol of the remote device works improperly, contact the engineer responsible for the remote device to rectify the fault. If the fault is rectified but the alarm is not cleared, go to Step 2.
 - b. Collect alarm information and configuration information, and then contact technical support personnel.
 - Cause 13: The PVC is Down.
 - a. Run the **display this** command in the sub-interface view to check whether the interfaces on both ends are shut down.
 - If the interfaces are shut down, go to Step 4.
 - If the interfaces are not shut down, go to Step 2.
 - b. Run the **display fr interface** command in the system view to check the physical and protocol status of the main interface.
 - If the physical status of the main interface is Down, go to Step 5.

- If the physical status of the main interface is Up but the protocol status is Down, go to Step 6.
 - If the both the physical and protocol status of the main interface is Up, go to Step 3.
 - c. Ask engineers of the peer end to check whether the PVC status is Active.
 - If the PVC status on the peer end is Active, go to Step 7.
 - If the PVC status on the peer end is Inactive, go to Step 8.
 - d. Run the **undo shutdown** command to start the sub-interface.
 - e. Check the physical connection of the main interface.
 - f. Check the LMI configurations.
 - g. Collect alarm information and configuration information, and then contact technical support personnel.
 - h. End.
- Cause 14: EFM DOWN.
 - a. Run the **display efm session** command in the system view to check whether the EFM state field is displayed as Detect.
 - If the EFM state field is displayed as Detect, go to Step 3.
 - If the EFM state field is not displayed as Detect, go to Step 2.
 - b. Run the **display efm** command in the system view to check whether the EFM enable flag field is displayed as enabled.
 - If the EFM enable flag field is displayed as enabled, recheck the physical link and then check whether the alarm is cleared. If the alarm is not cleared, go to Step 3.
 - If EFM enable flag is not enabled, run the **efm enable** command in the system view and interface view according to the configuration guide. Then check whether the alarm is cleared. If the alarm persists, go to Step 3.
- 3. Collect alarm information and configuration information, and then contact technical support personnel.
- Cause 15: The tunnel is down.
 - a. Run the **display interface** command in the system view to check whether the tunnel link is Down.
 - If the physical status of the interface is Down, run the **undo shutdown** command to enable the interface and check whether the alarm is cleared. If the alarm persists, go to Step 2.
 - If the physical status of the interface is Up, go to step 3.
 - b. Check whether the physical link is normal, for example, whether the network cable or optical module is loose or disconnected.
 - If the physical link is abnormal, reconnect the physical link and check whether the alarm is cleared. If the alarm persists, go to Step 3.

- If the physical link works properly, go to Step 3.
- c. Run the **display this** command in the interface view to check whether MPLS TE and MPLS RSVP-TE are configured on the tunnel interface and nodes.
 - If MPLS TE and MPLS RSVP-TE are configured on the tunnel link interface and node, go to Step 4.
 - If MPLS TE and MPLS RSVP-TE are not configured on the tunnel interface or node, run the **mpls te** and **mpls rsvp-te** commands in the MPLS view to reconfigure them. Then, check whether the alarm is cleared. If the alarm persists, go to Step 4.
- d. Collect alarm and configuration information, and contact technical support personnel.
- Cause 16: The interface is shut down.
 - a. Run the **display this** command in the interface view to check whether the interfaces at both ends are shut down. If the interfaces are sub-interfaces, check whether VLAN IDs are configured for the interfaces at both ends.
 - If the interface is a sub-interface, run the **vlan-type dot1q** command to configure a correct VLAN ID for the sub-interface. Then, check whether the alarm is cleared. If the alarm persists, go to Step 2.
 - If the interface is not shut down, go to Step 2.
 - 2. Collect alarm and configuration information, and contact technical support personnel.
- Cause 17: The link protocol is down.
 - a. Run the **display this** command in the interface view to check whether the interfaces at both ends are shut down. If the interfaces are sub-interfaces, check whether VLAN IDs are configured for the interfaces at both ends.
 - If the interface is a sub-interface, run the **vlan-type dot1q** command to configure a correct VLAN ID for the sub-interface. Then, check whether the alarm is cleared. If the alarm persists, go to Step 2.
 - If the interface is not shut down, go to Step 2.
 - b. Check the cause of the protocol Down event based on the corresponding link layer protocol.
 - If the link layer protocol can go Up, the fault is rectified.
 - If the link layer protocol still cannot go Up, go to Step 3.
 - c. Collect alarm and configuration information, and contact technical support personnel.
- Cause 19: The link protocol is up.

This alarm message is informational only, and no action is required.
- Cause 20: The main interface is down.

- a. Run the **display this** command in the interface view to check whether the interface on each end is shut down.
 - If the interface is shut down, run the **undo shutdown** command to enable the interface. After that, check whether the alarm is cleared. If the alarm is not cleared, go to Step 2.
 - If the interface is not shut down, go to Step 2.
 - b. Check whether the physical link of the interface works improperly. That is, check whether the hardware such as the network cable or optical module is disconnected or loosely connected.
 - If the physical link works improperly, you need to correctly connect the physical link and then check whether the alarm is cleared. If the alarm is not cleared, go to Step 3.
 - If the physical link works properly, go to Step 3.
3. Collect alarm information and configuration information, and then contact technical support personnel.
- Cause 21: Interface physical link is up.
This alarm message is informational only, and no action is required.
 - Cause 22: The conditions for the activation of the interface are not met.
 - a. Run the **display interface** command in the system view to check whether the physical statuses of the local and remote interfaces are Up.
 - If physical statuses of the local and remote interfaces are Down, run the **undo shutdown** command in the interface view to enable the interface, and then check whether the alarm is cleared. If the alarm is not cleared, go to Step 2.
 - If physical statuses of the local and remote interfaces are Up, go to Step 2.
 - b. Run the **display eth-trunk** command in the system view to check whether the number of trunk member interfaces on the local and remote ends is larger than the max active-linkup number.
 - If the number is larger than the max active-linkup number, it indicates a normal situation in the LACP protocol negotiation process, and no action is required.
 - If the number is smaller than the max active-linkup number, go to Step 3.
 - c. Run the **display eth-trunk** command in the system view to check whether the number of trunk member interfaces on the local and remote ends is smaller than least active-linkup number.
 - If the number of trunk member interfaces on the local and remote ends is less than least active-linkup number, run the **least active-linknumber** command to change least active-linkup number so that the former is greater than or equal to the latter.
 - If the number of trunk member interfaces on the local and remote ends is greater than least active-linkup number, go to Step 4.

4. Collect alarm information and configuration information, and then contact technical support personnel.

- Cause 23: The conditions for the activation of the interface are met.
This alarm message is informational only, and no action is required.
- Cause 24: The tunnel is up.
This alarm message is informational only, and no action is required.
- Cause 25: The interface is deleted.
Usually, it was because a user had deleted a logical interface. This alarm message is informational only, and no action is required.
- Cause 26: BFD session is down.
 - a. Run the **display bfd session** command in the system view to check BFD session information.
 - If the interface is bound to a BFD session and the BFD session is in the Down state, refer to the BFD troubleshooting guide and rectify the fault.
 - If the interface is bound to a BFD session and the BFD session is in the Up state, go to Step 2.

2. Collect alarm information and configuration information, and then contact technical support personnel.

- Cause 27: BFD session is up.
This alarm message is informational only, and no action is required.
- Cause 28: EFM UP.
This alarm message is informational only, and no action is required.
- Cause 30: DLDP detect down.
 - a. Check the traps to determine the fault cause.
 - b. Check the possible causes.
- Cause 31: DLDP detect up.
This alarm message is informational only, and no action is required.
- Cause 32: VRRP FLOW DOWN.
 - a. Run the **display vrrp** command in the system view to check VRRP information.
 - If the mVRRP backup group is Down, refer to the VRRP troubleshooting guide and rectify the fault.
 - If the mVRRP backup group is Up, go to Step 2.
 - b. Collect alarm information and configuration information, and then contact technical support personnel.
- Cause 33: VRRP FLOW UP.
This alarm message is informational only, and no action is required.
- Cause 34: VE FLOW DOWN.
 - a. Run the **display interface virtual-ethernet ve-number** command to check VE interface information.

- If the VE interface is Down, go to Step 2.
 - If the VE interface is Up, go to Step 4.
 - b. Collect the main interface configuration.
 - If it matches the L2VPN termination interface, see the L2VPN troubleshooting guide and rectify the fault.
 - If it matches the L3VPN termination interface, go to Step 3.
 - c. Collect the L3VPN termination sub-interface configuration, and check whether the sub-interface has a VLAN ID and IPv4 address configured.
 - If the configuration is not correct, go to Step 4.
 - If the configuration is correct but the alarm persists, go to Step 4.
 - d. Collect alarm information and configuration information, and then contact technical support personnel.
- Cause 35: VE FLOW UP.

This alarm message is informational only, and no action is required.
- Cause 36: The interface is error down.

For details about handling suggestions, see "ERROR-DOWN_1.3.6.1.4.1.2011.5.25.257.2.1 hwErrordown" Handling Procedure.
- Cause 37: CRC ERR DOWN.
 - a. Run the **display interface [interface-type [interface-number] | slot slot-number]** command to check the status of the link layer protocol on the interface.
 - If the status of the link layer protocol on the interfaces is Up (Bit-error-detection down), BER exceeds the BER alarm threshold, go to Step 2.
 - If the status of the link layer protocol on the interfaces is Down (Bit-error-detection down), go to Step 3.
 - b. Check whether the physical link of the interface works improperly. That is, check whether the hardware such as the network cable or optical module is disconnected or loosely connected.
 - If the physical link works improperly, you need to correctly connect the physical link and then check whether the alarm is cleared. If the alarm is not cleared, go to Step 3.
 - If the physical link works properly, go to Step 3.
 - c. Collect alarm information and configuration information, and then contact technical support personnel.
- Cause 38: CRC ERR UP.

This alarm message is informational only, and no action is required.
- Cause 39: Transceiver speed does not match the speed configured on the port.
 - a. Delete the speed configuration on the port and check whether the alarm is cleared. If the alarm persists, go to Step 2.

- b. Check whether the physical link of the interface works improperly. That is, check whether the hardware such as the network cable or optical module is disconnected or loosely connected.
 - If the physical link works improperly, you need to correctly connect the physical link and then check whether the alarm is cleared. If the alarm is not cleared, go to Step 3.
 - If the physical link works properly, go to Step 3.
 - c. Collect alarm information and configuration information, and then contact technical support personnel.
- Cause 40: The port does not support current transceiver.
 - a. Replace the current transceiver with a transceiver that the port supports and check whether the alarm is cleared. If the alarm persists, go to Step 2.
 - b. Check whether the physical link of the interface works improperly. That is, check whether the hardware such as the network cable or optical module is disconnected or loosely connected.
 - If the physical link works improperly, you need to correctly connect the physical link and then check whether the alarm is cleared. If the alarm is not cleared, go to Step 3.
 - If the physical link works properly, go to Step 3.
 - c. Collect alarm information and configuration information, and then contact technical support personnel.
- Cause 41: Transceiver does not support the negotiation configuration on the port.
 - a. Delete the negotiation configuration on the port and check whether the alarm is cleared. If the alarm persists, go to Step 2.
 - b. Check whether the physical link of the interface works improperly. That is, check whether the hardware such as the network cable or optical module is disconnected or loosely connected.
 - If the physical link works improperly, you need to correctly connect the physical link and then check whether the alarm is cleared. If the alarm is not cleared, go to Step 3.
 - If the physical link works properly, go to Step 3.
 - c. Collect alarm information and configuration information, and then contact technical support personnel.
- Cause 43: The interface is trigger down.
 - a. Run the **display interface [interface-type [interface-number] | slot slot-number]** command and check whether the specified interface status is TRIGGER DOWN.
 - If the interface status is TRIGGER DOWN, go to Step 2.
 - If the interface status is not TRIGGER DOWN, go to Step 4.
 - b. Check the cause following the TRIGGER DOWN field and view the associated service, for example, TRIGGER DOWN (MONITOR GROUP).

- If a cause is displayed, go to Step 3.
- If no cause is displayed, go to Step 4.
- c. Check and restore the associated service. Check whether the trap is cleared. If the trap persists, go to Step 4.
- d. Collect alarm information and configuration information, and then contact technical support personnel.
- Cause 48: CFM DOWN.
 - a. Check the CFM status information.
 - If the CFM status is normal, go to Step 2.
 - If the CFM status is abnormal, see CFM-related troubleshooting.
 - b. Please Collect alarm information and configuration information, and then contact technical support personnel.
- Cause 49: CFM UP.

This alarm message is informational only, and no action is required.
- Cause 51: The sub-interface linkDown alarm is disabled.

This alarm message is informational only, and no action is required.

Clearing

After the fault is rectified, the system clears this alarm, removing the need to manually clear it. This alarm will not be displayed on the **CurrentAlarms** page.

3.5.1.8 ALM-135462958 hwBoardInvalid

Description

The board totally failed. (EntPhysicalIndex=[EntPhysicalIndex], EntPhysicalName=[EntPhysicalName], EntityType=[EntityType], EntityTrapFaultID=[EntityTrapFaultID], Reason=[Reason])

A board experienced a complete failure.

Attribute

Alarm ID	OID	Alarm Severity	Alarm Type
135462958	1.3.6.1.4.1.2011.5.25.219.2.2.5	Critical	Equipment alarm

Parameters

Name	Meaning
EntPhysicalIndex	Entity index.

Name	Meaning
EntPhysicalName	Entity name.
EntityType	Entity type.
EntityTrapFaultID	Alarm cause.
Reason	

Impact on the System

- Cause 1: The power supplied to the board is insufficient.
The board completely fails, and services are interrupted.
- Cause 6: The EPLD logic of the board failed.
The board completely fails, and services are interrupted.
- Cause 7: The in-position board type conflicts with the pre-configured board type.
The board completely fails, and services are interrupted.
- Cause 8: The clock signals of the board were incorrect.
The board completely fails, and services are interrupted.
- Cause 9: The board does not support some configurations and cannot register.
The board completely fails, and services are interrupted.
- Cause 10: The board does not match the device.
The board completely fails, and services are interrupted.
- Cause 11: The FPGA local bus self-check failed.
The board completely fails, and services are interrupted.
- Cause 12: The SD5K communication failed.
The board completely fails, and services are interrupted.
- Cause 13: The board obtained abnormal signals from the master and slave MPUs.
The board completely fails, and services are interrupted.
- Cause 14: The device hardware verification failed.
The board completely fails, and services are interrupted. Key components of the board may have been replaced or tampered with, affecting system reliability and security.
- Cause 19: TCAM chip failed.
The board completely fails, and services are interrupted.
- Cause 20: The FPGA entry of the board may be faulty.
The board completely fails, and services are interrupted.
- Cause 21: The PCIE of the board was faulty.
The board completely fails, and services are interrupted.
- Cause 22: The board is not installed properly.
The board completely fails, and services are interrupted.

- Cause 23: The PCIE link of the FPGA and slave CXP is faulty.
The board completely fails, and services are interrupted.
- Cause 24: Board burnt due to high PoE power.
The board completely fails, and services are interrupted.
- Cause 26: The master or slave ACT signal of the MPU board is abnormal.
The services on the board may be affected or even interrupted. Therefore, the problem needs to be solved immediately.
- Cause 33: The board was not registered.
The board completely fails, and services are interrupted.
- Cause 66: The board failed to register after three registration attempts.
The board completely fails, and services are interrupted.
- Cause 67: A board was powered off. Possible causes include: The board was manually powered off; the current version does not support this board; the board temperature was too high; the board was not registered for a long period of time; the board was not working normally.
The board completely fails, and services are interrupted.
- Cause 68: The board was powered on.
There is no impact.
- Cause 69: The FPGA of the board failed.
The board completely fails, and services are interrupted.
- Cause 70: The board does not match the slot.
The board completely fails, and services are interrupted.
- Cause 80: The power supply self-check failed.
The board completely fails, and services are interrupted.
- Cause 85: The smi serial of the board is abnormal.
The board completely fails, and services are interrupted.
- Cause 87: The card failed to be registered.
The board completely fails, and services are interrupted.
- Cause 98: The EPLD logic of the board failed.
The services on the board may be affected or even interrupted. Therefore, the problem needs to be solved immediately.
- Cause 99: The FPGA local bus self-check failed.
The board completely fails, and services are interrupted.
- Cause 123: The board voltage exceeded the major alarm threshold.
The board completely fails, and services are interrupted.
- Cause 124: The board voltage fell below the major alarm threshold.
The board completely fails, and services are interrupted.
- Cause 125: The board voltage exceeds the fatal alarm threshold.
The board completely fails, and services are interrupted.
- Cause 126: The board voltage fell below the fatal alarm threshold.
The board completely fails, and services are interrupted.

- Cause 127: The board is incompatible with the software version.
The services on the board may be affected or even interrupted. Therefore, the problem needs to be solved immediately.
- Cause 128: Different SFUs were installed in the same chassis.
The board completely fails, and services are interrupted.
- Cause 130: The card is incompatible with board.
The subcard fails, and services are interrupted.

Possible Causes

- Cause 1: The power supplied to the board is insufficient.
- Cause 6: The EPLD logic of the board failed.
- Cause 7: The in-position board type conflicts with the pre-configured board type.
- Cause 8: The clock signals of the board were incorrect.
- Cause 9: The board does not support some configurations and cannot register.
- Cause 10: The board does not match the device.
- Cause 11: The FPGA local bus self-check failed.
- Cause 12: The SD5K communication failed.
- Cause 13: The board obtained abnormal signals from the master and slave MPUs.
- Cause 14: The device hardware verification failed.
- Cause 19: TCAM chip failed.
- Cause 20: The FPGA entry of the board may be faulty.
- Cause 21: The PCIE of the board was faulty.
- Cause 22: The board is not installed properly.
- Cause 23: The PCIE link of the FPGA and slave CXP is faulty.
- Cause 24: Board burnt due to high PoE power.
- Cause 26: The master or slave ACT signal of the MPU board is abnormal.
- Cause 33: The board was not registered.
- Cause 66: The board failed to register after three registration attempts.
- Cause 67: A board was powered off. Possible causes include:
 - The board was manually powered off.
 - The current version does not support this board.
 - The board temperature was too high.
 - The board was not registered for a long period of time.
 - The board was not working normally.
- Cause 68: The board was powered on.
- Cause 69: The FPGA of the board failed.
- Cause 70: The board does not match the slot.
- Cause 80: The power supply self-check failed.
- Cause 85: The smi serial of the board is abnormal.

- Cause 87: The card failed to be registered.
- Cause 98: The EPLD logic of the board failed.
- Cause 99: The FPGA local bus self-check failed.
- Cause 123: The board voltage exceeded the major alarm threshold.
- Cause 124: The board voltage fell below the major alarm threshold.
- Cause 125: The board voltage exceeds the fatal alarm threshold.
- Cause 126: The board voltage fell below the fatal alarm threshold.
- Cause 127: The board is incompatible with the software version.
- Cause 128: Different SFUs were installed in the same chassis.
- Cause 130: The card is incompatible with board.

Procedure

- Cause 1: The power supplied to the board is insufficient.
 - a. Collect trap, log, and configuration information, and contact technical support.
- Cause 6: The EPLD logic of the board failed.
 - a. Check whether the faulty board is the active board.
 - If yes, perform the active/standby switchover when the standby board is normal.
 - If not, go to 2.
 - b. Power off and then power on the faulty board. If the faulty board cannot be registered or the fault persists after the board is registered, replace the faulty board.
- Cause 7: The in-position board type conflicts with the pre-configured board type.
 - a. Change the pre-configured conflict policy to be based on the physical configuration.
 - b. Delete the pre-configured board configuration at the position.
 - c. Remove the board.
 - d. Clear the offline configuration of the slot.
- Cause 8: The clock signals of the board were incorrect.
 - a. Check whether the faulty board is reset or powered off and whether services are running properly.
 - If the board is not reset or powered off and services are running properly, go to 4.
 - If the board is reset or powered off, or services are abnormal, go to 2.
 - b. Power off and then power on the faulty board.
 - If the board registers successfully and the fault is rectified after the registration, go to 5.

- If the board cannot be registered or the alarm persists after the board is registered, go to 3.
 - c. Replace the fault board.
 - If the board registers successfully and the fault is rectified after the registration, go to 5.
 - If the board cannot be registered or the alarm persists after the board is registered, go to 4.
 - d. Contact technical support personnel.
 - e. End.
- Cause 9: The board does not support some configurations and cannot register.
 - a. The current system does not support the board. Remove the board.
- Cause 10: The board does not match the device.
 - a. The current subrack does not support the board. Remove the board.
- Cause 11: The FPGA local bus self-check failed.
 - a. If the faulty board is not the active main control board, go to 3.
 - b. If the slave main control board is normal, run the slave switchover command in the system view to perform a master/slave main control board switchover. Then go to 1.
 - c. Power off and then power on the faulty board.
 - d. If the fault persists, replace the faulty board.
- Cause 12: The SD5K communication failed.
 - a. Collect alarm, log, and configuration information, and contact technical support personnel.
- Cause 13: The board obtained abnormal signals from the master and slave MPUs.
 - a. Check whether the two MPUs are installed properly. If not, install them properly and check whether the fault is rectified.
 - If the fault is rectified, go to step 4.
 - If the fault persists, go to step 2.
 - b. If services are not running on the faulty board, perform the following operations. If the fault is rectified, go to step 4. Otherwise, go to step 3.
 - If the board is not properly installed, install it properly.
 - If the backplane has bent pins, do not insert the new board into the faulty slot and contact Huawei technical support personnel.
 - If the board connector is faulty, replace the board.
 - c. If services are running on the faulty board or the fault persists, contact technical support personnel.
 - d. End.
- Cause 14: The device hardware verification failed.

- a. Reset the board and check whether the fault is rectified. If the fault persists, replace the board.
- Cause 19: TCAM chip failed.
 - a. Check whether the faulty board is reset or powered off and whether services are running properly.
 - If the board is not reset or powered off and services are running properly, go to 4.
 - If the board is reset or powered off, or services are abnormal, go to 2.
 - b. Power off and then power on the faulty board.
 - If the board registers successfully and the fault is rectified after the registration, go to 5.
 - If the board cannot be registered or the alarm persists after the board is registered, go to 3.
 - c. Replace the faulty board.
 - If the board registers successfully and the fault is rectified after the registration, go to 5.
 - If the board cannot be registered or the alarm persists after the board is registered, go to 4.
 - d. Contact technical support.
 - e. End
- Cause 20: The FPGA entry of the board may be faulty.
 - a. Check whether the faulty board is reset or powered off and whether services are running properly.
 - If the board is not reset or powered off and services are running properly, go to 4.
 - If the board is reset or powered off, or services are abnormal, go to 2.
 - b. Power off and then power on the faulty board.
 - If the board registers successfully and the fault is rectified after the registration, go to 5.
 - If the board cannot be registered or the alarm persists after the board is registered, go to 3.
 - c. Replace the faulty board.
 - If the board registers successfully and the fault is rectified after the registration, go to 5.
 - If the board cannot be registered or the alarm persists after the board is registered, go to 4.
 - d. Contact technical support.
 - e. End.

- Cause 21: The PCIE of the board was faulty.
 - a. Check whether the faulty board is reset or powered off and whether services are running properly.
 - If the board is not reset or powered off and services are running properly, go to 4.
 - If the board is reset or powered off, or services are abnormal, go to 2.
 - b. Power off and then power on the faulty board.
 - If the board registers successfully and the fault is rectified after the registration, go to 5.
 - If the board cannot be registered or the alarm persists after the board is registered, go to 3.
 - c. Replace the faulty board.
 - If the board registers successfully and the fault is rectified after the registration, go to 5.
 - If the board cannot be registered or the alarm persists after the board is registered, go to 4.
 - d. Contact technical support.
 - e. End.
- Cause 22: The board is not installed properly.
 - a. Check whether the line card is installed properly. If not, install the line card properly and check whether the fault is rectified. If the alarm persists, go to 2.
 - b. Collect trap, log, and configuration information, and contact technical support.
- Cause 23: The PCIE link of the FPGA and slave CXP is faulty.
 - a. Collect alarm, log, and configuration information, and contact technical support personnel.
- Cause 24: Board burnt due to high PoE power.
 - a. Collect trap and log information, and contact Huawei technical support.
- Cause 26: The master or slave ACT signal of the MPU board is abnormal.
 - a. Check whether other boards have low voltage alarms or power-related alarms. If so, clear the alarms first.
 - b. Remove and reinstall the current standby main control board. Check whether the board is properly installed, whether there are bent pins, and whether the board connector is faulty. If so, go to step 4.
 - c. If the device is reset, remove the other main control board and check whether the main control board is properly installed, whether there are bent pins, and whether the board connector is faulty. If so, go to step 4.
 - d. If the board is not properly inserted, insert the board properly.
 - e. If the backplane has bent pins, do not insert a new board into the slot and contact the technical support personnel.

- f. If only the connector of the faulty board is faulty, replace the board and go to step 8.
 - g. If the standby main control board is not registered or the alarm persists, contact the technical support personnel.
 - h. End.
- Cause 33: The board was not registered.
 - a. Collect trap, log, and configuration information, and contact technical support.
- Cause 66: The board failed to register after three registration attempts.
 - a. Collect alarm, log, and configuration information, and contact technical support.
- Cause 67: A board was powered off.
 - a. Replace the board and check whether the alarm is cleared. If the alarm persists, go to 2.
 - b. Collect trap, log, and configuration information, and contact technical support.
- Cause 68: The board was powered on.
 - a. The board is powered on.
- Cause 69: The FPGA of the board failed.
 - a. Determine the slot ID of the faulty board based on EntPhysicalName. The first digit after fpga indicates the FPGA chip ID, and the second and subsequent digits indicate the slot ID of the board. For example, EntPhysicalName=fpga1 3 indicates that FPGA1 in slot 3 is faulty.
 - b. If the faulty board cannot be registered after being restarted or the alarm cannot be cleared after being registered, replace the faulty board.
 - c. If the faulty board is not restarted or powered off and services are running properly, contact technical support personnel.
- Cause 70: The board does not match the slot.
 - a. The current slot does not support the board. Remove the board.
- Cause 80: The power supply self-check failed.
 - a. Collect trap, log, and configuration information, and contact technical support.
- Cause 85: The smi serial of the board is abnormal.
 - a. Collect alarm, log, and configuration information, and contact technical support personnel.
- Cause 87: The card failed to be registered.
 - a. Remove and then insert the subcard. If the faulty subcard still cannot be registered, replace the faulty subcard and check whether the fault is rectified. If the alarm persists, go to step 2.
 - b. Collect alarm, log, and configuration information, and contact technical support.
- Cause 98: The EPLD logic of the board failed.
 - a. If the faulty board is not the active main control board, go to Step 3.

- b. If the standby main control board is normal, perform an active/standby switchover in the system view and go to Step 1.
 - c. If the faulty board is already registered, run the upgrade mpu/lpu/sfu <slotid> startup firmware command in the user view to upgrade the CPID, and go to Step 5.
 - d. If the faulty board is not registered, power off and then power on the board.
 - e. If the faulty board cannot be registered or the fault persists after registration, replace the faulty board.
- Cause 99: The FPGA local bus self-check failed.
 - a. Collect alarm, log, and configuration information, and contact technical support.
- Cause 123: The board voltage exceeded the major alarm threshold.
 - a. Collect trap, log, and configuration information, and contact technical support.
- Cause 124: The board voltage fell below the major alarm threshold.
 - a. Collect trap, log, and configuration information, and contact technical support.
- Cause 125: The board voltage exceeds the fatal alarm threshold.
 - a. Collect alarm, log, and configuration information, and contact technical support personnel.
- Cause 126: The board voltage fell below the fatal alarm threshold.
 - a. Collect alarm, log, and configuration information, and contact technical support personnel.
- Cause 127: The board is incompatible with the software version.
 - a. Collect alarm, log, and configuration information, and contact technical support.
- Cause 128: Different SFUs were installed in the same chassis.
 - a. Run the clear inactive-configuration command to clear the offline configuration.
 - b. Remove and then insert the faulty board or power on the faulty board. Then, check whether the fault is rectified.
 - If the fault is rectified, go to Step 4.
 - If the fault persists, go to Step 3.
 - c. Collect alarm, log, and configuration information, and contact technical support.
 - d. End.
- Cause 130: The card is incompatible with board.
 - a. Remove the subcard and install a subcard that is compatible with the board type.

Clearing

After the fault is rectified, the system clears this alarm, removing the need to manually clear it. This alarm will not be displayed on the **CurrentAlarms** page.

3.5.1.9 ALM-135462935 hwFanInvalid

Description

A fan module experienced a complete failure.
(EntPhysicalIndex=[EntPhysicalIndex], EntPhysicalName=[EntPhysicalName], EntityTrapFaultID=[EntityTrapFaultID], EntityOperStatus=[EntityOperStatus], Reason=[ReasonDsp])

A fan module experienced a complete failure.

Attribute

Alarm ID	OID	Alarm Severity	Alarm Type
135462935	1.3.6.1.4.1.2011.5.2 5.219.2.6.5	Major	Equipment alarm

Parameters

Name	Meaning
EntPhysicalIndex	Entity index.
EntPhysicalName	Entity Name
EntityTrapFaultID	Fault Code
EntityOperStatus	Alarm status information
ReasonDsp	Alarm cause

Impact on the System

The heat dissipation performance of the device is affected, but the temperature of the device increases. Services are not affected in a short period of time, but the fault needs to be rectified immediately.

Possible Causes

- Cause 1: Fan communicate with MPU is failed.
- Cause 2: The fans in the fan module failed.
- Cause 3: The fan was not present.
- Cause 4: This fan module is not recommended because it may cause insufficient heat dissipation.

- Cause 5: The fan type is mismatch with the device.

Procedure

- Cause 1: Fan communicate with MPU is failed.
Collect trap, log, and configuration information, and contact technical support personnel.
- Cause 2: The fans in the fan module failed.
Collect trap, log, and configuration information, and contact technical support personnel.
- Cause 3: The fan was not present.
Insert the fan.
- Cause 4: This fan module is not recommended because it may cause insufficient heat dissipation.
Replace the fan with the recommended one.
- Cause 5: The fan type is mismatch with the device.
Replace the fan to ensure that the fan matches the device.

Clearing

After the fault is rectified, the system clears this alarm, removing the need to manually clear it. This alarm will not be displayed on the **CurrentAlarms** page.

3.5.1.10 ALM-135462966 hwFanFail

Description

The fan partially failed. (EntPhysicalIndex=[EntPhysicalIndex], EntPhysicalName=[EntPhysicalName], EntityTrapFaultID=[EntityTrapFaultID], EntityOperStatus=[EntityOperStatus], Reason=[ReasonDsp])

The fan partially failed.

Attribute

Alarm ID	OID	Alarm Severity	Alarm Type
135462966	1.3.6.1.4.1.2011.5.25.219.2.6.3	Major	Equipment alarm

Parameters

Name	Meaning
EntPhysicalIndex	Indicates the entity index.
EntPhysicalName	Indicates the entity name.

Name	Meaning
EntityTrapFaultID	Indicates the error code.
EntityOperStatus	Indicates the Status.
ReasonDsp	Indicates a possible cause.

Impact on the System

A fault of the fan module affects heat dissipation performance of the switch.
Services are not affected in a short time, but you need to rectify the fault quickly.

Possible Causes

- Cause 1: The fan module was in abnormal state.
- Cause 2: The fan wind direction was abnormal.

Procedure

1. Replace the fan module.
2. If the problem persists, collect alarm, log, and configuration information, and contact technical support personnel.

Clearing

After the fault is rectified, the system clears this alarm, removing the need to manually clear it. This alarm will not be displayed on the **Current Alarms** page.

3.5.1.11 ALM-15795007 hwPKILocalCertInvalid

Description

PKI/2/PKILOCALCERTINVALID: OID [*oid*] the local certificate is invalid.
(LocalCertIssuer=[*issuer*], LocalCertSubject=[*subject*],
LocalCertStartTime=[*starttime*], LocalCertFinishTime=[*finishtime*])

The local certificate is invalid.

Attribute

Alarm ID	OID	Alarm Severity	Alarm Type
15795007	1.3.6.1.4.1.201 1.6.122.34.0.2. 12	Major	Communication alarm

Parameters

Name	Meaning
oid	Indicates the MIB object ID of the alarm.
issuer	Indicates the issuer of the local certificate.
subject	Indicates the subject of the local certificate.
starttime	Indicates the start time of the local certificate.
finishtime	Indicates the end time of the local certificate.

Impact on the System

The service becomes invalid.

Possible Causes

The local certificate is invalid.

Procedure

- Step 1 Check whether the system time on the local device is correct.
 - Step 2 If the system time is correct, apply for a new local certificate.
- End

Clearing

The alarm needs to be cleared manually.

3.5.1.12 ALM-135463086 hwIfMonitorInputRateRising

Description

Interface input flow bandwidth usage exceeded the trap threshold.
(Interface=[IfIndex], BandWidthUsage=[hwIfMonitorInputRatePercentage],
TrapThreshold=[hwIfMonitorInputRateThreshold],
InterfaceName=[InterfaceName])

This object indicates that an alarm is generated when the percentage of the traffic received by an interface to the total bandwidth of the interface exceeds the threshold.

Attribute

AlarmID	Alarm OID	Alarm Severity	Alarm Type
135463086	1.3.6.1.4.1.2011.5.25.41.4.5	Warning	Processing error alarm

Parameters

Parameter	Description
IfIndex	Interface index
hwIfMonitorInputRatePercentage	Input traffic statistics.
hwIfMonitorInputRateThreshold	Input traffic alarm threshold.
InterfaceName	Interface name.

Impact on the System

When the traffic is close to 100% of the bandwidth, delay or packet loss may occur.

Possible Causes

The rate of traffic received by the interface was too large.

Procedure

1. Run the **display this interface** command in the interface view to check whether the traffic threshold is too low. Determine the alarm threshold based on service requirements.

- If yes, go to Step 2.
- If not, go to Step 3.

2. Run the **trap-threshold input-rate *bandwidth-in-use*** command in the interface view to reconfigure the alarm threshold. Then check whether the alarm is cleared.

- If yes, go to Step 4.
- If not, go to Step 3.

3. Collect alarm and configuration information, and contact technical support personnel.

4. End.

Related Information

None.

3.5.1.13 ALM-135463087 hwIfMonitorOutputRateRising

Description

Interface output flow bandwidth usage exceeded the trap threshold.
(Interface=[IfIndex], BandWidthUsage=[hwIfMonitorOutputRatePercentage],
TrapThreshold=[hwIfMonitorOutputRateThreshold],
InterfaceName=[InterfaceName])

This object indicates that an alarm is generated when the ratio of the traffic sent by an interface to the total bandwidth of the interface exceeds the threshold.

Attribute

AlarmID	Alarm OID	Alarm Severity	Alarm Type
135463087	1.3.6.1.4.1.2011.5.25 .41.4.7	Warning	Processing error alarm

Parameters

Parameter	Description
IfIndex	Interface index
hwIfMonitorOutputRatePercentage	Output traffic statistics.
hwIfMonitorOutputRateThreshold	Output traffic alarm threshold.
InterfaceName	Interface name.

Impact on the System

When the traffic is close to 100% of the bandwidth, delay or packet loss may occur.

Possible Causes

The rate of traffic sent by the interface was too large.

Procedure

1. Run the **display this interface** command in the interface view to check whether the traffic threshold is too low. Determine the alarm threshold based on service requirements.

- If yes, go to step 2.
- If not, go to Step 3.

2. Run the **trap-threshold output-rate *bandwidth-in-use*** command in the interface view to reconfigure the alarm threshold. Then check whether the alarm is cleared.
- If yes, go to Step 4.
 - If not, go to Step 3.
3. Collect alarm and configuration information, and contact technical support personnel.
4. End.

Related Information

None.

3.5.1.14 ALM-135471444 hwOpticalUnauthorized

Description

The optical module was not certified by Huawei.
(EntPhysicalIndex=[EntPhysicalIndex], EntPhysicalName=[EntPhysicalName], EntityTrapFaultID=[EntityTrapFaultID], Reason=[Reason])

The optical module is not a Huawei certified one.

Attribute

AlarmID	Alarm OID	Alarm Severity	Alarm Type
135471444	1.3.6.1.4.1.2011.5.25.219.2.4.9	Critical	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
EntPhysicalIndex	Entity index.
EntPhysicalName	Entity Name
EntityTrapFaultID	Alarm cause
Reason	

Impact on the System

If the optical module is delivered by Huawei in the early stage, the system is not affected. If not, the optical module may be abnormal, causing service interruption.

Possible Causes

An optical module that is not certified for Huawei was installed. Alarms may be generated because vendor information of Huawei early delivered optical modules is not recorded.

Procedure

1. If the optical modules are early delivered from Huawei, run the **transceiver non-certified-alarm disable** command to disable the alarm function for non-Huawei-certified optical modules.
2. If the optical module is not delivered by Huawei or is not a Huawei-certified optical module, replace it with a Huawei-certified optical module.

Related Information

None.

3.5.1.15 ALM-135463001 hwOpticalInvalid

Description

Optical Module is invalid. (EntPhysicalIndex=[EntPhysicalIndex], EntPhysicalName=[EntPhysicalName], EntityTrapFaultID=[EntityTrapFaultID], Reason=[Reason])

An optical module was faulty.

Attribute

AlarmID	Alarm OID	Alarm Severity	Alarm Type
135463001	1.3.6.1.4.1.2011.5.25.219.2.4.5	Minor	Equipment alarm

Parameters

Parameter	Description
EntPhysicalIndex	Entity index.
EntPhysicalName	Entity name.
EntityTrapFaultID	Alarm cause.

Parameter	Description
Reason	

Impact on the System

- Cause 2: Output Optical Power Too High.
Services on the optical module may be affected, which may cause bit errors, error packets, or even service interruption.
- Cause 3: Output Optical Power Too Low.
Services on the optical module may be affected, which may cause bit errors, error packets, or even service interruption.
- Cause 4: Input Optical Power Too High.
Services on the optical module may be affected, which may cause bit errors, error packets, or even service interruption.
- Cause 5: Input Optical Power Too Low.
Services on the optical module may be affected, which may cause bit errors, error packets, or even service interruption.
- Cause 7: The IIC of the optical module failed.
Services on the optical module may be affected, which may cause bit errors, error packets, or even service interruption.
- Cause 8: The optical signals received by the optical module were lost.
Services on the optical module may be affected, which may cause bit errors, error packets, or even service interruption.
- Cause 9: The electrical signals sent by the optical module were lost.
Services on the optical module may be affected, which may cause bit errors, error packets, or even service interruption.
- Cause 10: Loss of lock was detected in the receive direction by the optical module.
Services on the optical module may be affected, which may cause bit errors, error packets, or even service interruption.
- Cause 11: Loss of lock was detected in the transmit direction by the optical module.
Services on the optical module may be affected, which may cause bit errors, error packets, or even service interruption.
- Cause 12: The optical module failed to send signals.
Services on the optical module may be affected, which may cause bit errors, error packets, or even service interruption.
- Cause 13: The voltage of the optical module was too high.
Services may be interrupted.
- Cause 14: The voltage of the optical module was too low.
Services may be interrupted.
- Cause 15: The bias current of the optical module was too high.
Services may be interrupted.

- Cause 16: The bias current of the optical module was too low.
Services may be interrupted.
- Cause 17: The temperature of the optical module was too high.
Services may be interrupted.
- Cause 18: The temperature of the optical module was too low.
Services may be interrupted.
- Cause 19: The power current of the optical module is too high.
Services might be interrupted.

Possible Causes

- Cause 2: Output Optical Power Too High.
- Cause 3: Output Optical Power Too Low.
- Cause 4: Input Optical Power Too High.
- Cause 5: Input Optical Power Too Low.
- Cause 7: The IIC of the optical module failed.
- Cause 8: The optical signals received by the optical module were lost.
- Cause 9: The electrical signals sent by the optical module were lost.
- Cause 10: Loss of lock was detected in the receive direction by the optical module.
- Cause 11: Loss of lock was detected in the transmit direction by the optical module.
- Cause 12: The optical module failed to send signals.
- Cause 13: The voltage of the optical module was too high.
- Cause 14: The voltage of the optical module was too low.
- Cause 15: The bias current of the optical module was too high.
- Cause 16: The bias current of the optical module was too low.
- Cause 17: The temperature of the optical module was too high.
- Cause 18: The temperature of the optical module was too low.
- Cause 19: The power current of the optical module is too high.

Procedure

- Cause 2: Output Optical Power Too High.
 1. Run the display interface command in the user view to check whether the Tx power of the interface is within the allowed range.
 - If so, collect alarm, log, and configuration information, and contact technical support personnel.
 - If not, replace the optical module.
 2. If the alarm persists, collect alarm, log, and configuration information, and contact technical support personnel.
- Cause 3: Output Optical Power Too Low.
 1. Run the display interface command in the user view to check whether the Tx power of the interface is within the allowed range.

- If so, go to step 2.
 - If not, replace the optical module.
- 2. Collect alarm, log, and configuration information, and contact technical support personnel.
- Cause 4: Input Optical Power Too High.
 - 1. Run the display interface command in the user view to check whether the Rx power of the interface is within the allowed range.
 - If so, collect trap, log, and configuration information, and contact technical support personnel.
 - If not, go to step 2.
 - 2. Check whether an alarm indicating that the Tx power is too high is generated on the remote interface.
 - If so, clear the alarm on the remote interface first.
 - If not, go to step 3.
 - 3. Check whether the peer optical module matches the local optical module.
 - If not, replace the optical module with one that matches the peer optical module.
 - If so, go to step 4.
 - 4. Add an optical attenuator to the local end. It is recommended that the attenuation be increased by -5 dB.
 - 5. If the alarm persists, replace the optical module.
 - 6. If the alarm still persists, collect alarm, log, and configuration information, and contact technical support personnel.
- Cause 5: Input Optical Power Too Low.
 - 1. Run the display interface command in the user view to check whether the Rx power of the interface is within the allowed range.
 - If so, collect trap, log, and configuration information, and contact technical support personnel.
 - If not, go to step 2.
 - 2. If the peer interface is not Down and no alarm is generated, go to step 4.
 - 3. Rectify the fault and clear the alarm on the peer interface. If the alarm is cleared, no further action is required.
 - 4. Check whether the optical fiber is faulty. If so, replace the optical fiber.
 - 5. Check whether an alarm is generated on the local interface. If so, replace the optical module to rectify the fault.
 - 6. If the alarm persists after the optical module is replaced, collect alarm, log, and configuration information, and contact technical support personnel.
- Cause 7: The IIC of the optical module failed.
 - 1. Check whether the optical module is securely installed. If so, remove the optical module and check whether the port has bent pins or is damaged. Try replacing the optical module. If the fault persists, contact technical support personnel.
- Cause 8: The optical signals received by the optical module were lost.

Check whether the optical fiber is faulty. If so, replace the optical fiber. If the fault persists, collect alarm, log, and configuration information, and contact technical support personnel.

- Cause 9: The electrical signals sent by the optical module were lost.
Collect alarm, log, and configuration information, and contact technical support personnel.
- Cause 10: Loss of lock was detected in the receive direction by the optical module.
Collect alarm, log, and configuration information, and contact technical support personnel.
- Cause 11: Loss of lock was detected in the transmit direction by the optical module.
Collect alarm, log, and configuration information, and contact technical support personnel.
- Cause 12: The optical module failed to send signals.
Collect alarm, log, and configuration information, and contact technical support personnel.
- Cause 13: The voltage of the optical module was too high.
 1. Run the display alarm all command to check whether the hwPowerInvalid alarm is generated.
 - If so, go to step 2.
 - If not, go to step 3.
 2. Handle the power alarm and check whether the alarm is cleared.
 - If the alarm is cleared, go to step 8.
 - If the alarm persists, go to step 3.
 3. Check the voltage of the board where the optical module resides and check whether a voltage alarm is generated on the NMS.
 - If so, go to step 4.
 - If not, go to step 5.
 4. Handle the voltage alarm and check whether the alarm is cleared.
 - If the alarm is cleared, go to step 8.
 - If the alarm persists, go to step 5.
 5. Replace the optical module and check whether the alarm is cleared.
 - If the alarm is cleared, go to step 8.
 - If the alarm persists, go to step 6.
 6. Replace the board where the optical module resides and check whether the alarm is cleared.
 - If the alarm is cleared, go to step 8.
 - If the alarm persists, go to step 7.
 7. Collect alarm, log, and configuration information, and contact technical support engineers.
 8. End.
- Cause 14: The voltage of the optical module was too low.

1. Run the display alarm all command to check whether the hwPowerInvalid alarm is generated.
 - If so, go to step 2.
 - If not, go to step 3.
 2. Handle the power alarm and check whether the alarm is cleared.
 - If the alarm is cleared, go to step 8.
 - If the alarm persists, go to step 3.
 3. Check the voltage of the board where the optical module resides and check whether a voltage alarm is generated on the NMS.
 - If so, go to step 4.
 - If not, go to step 5.
 4. Handle the voltage alarm and check whether the alarm is cleared.
 - If the alarm is cleared, go to step 8.
 - If the alarm persists, go to step 5.
 5. Replace the optical module and check whether the alarm is cleared.
 - If the alarm is cleared, go to step 8.
 - If the alarm persists, go to step 6.
 6. Replace the board where the optical module resides and check whether the alarm is cleared.
 - If the alarm is cleared, go to step 8.
 - If the alarm persists, go to step 7.
 7. Collect alarm, log, and configuration information, and contact technical support engineers.
 8. End.
- Cause 15: The bias current of the optical module was too high.
 1. Run the display alarm all command to check whether the hwPowerInvalid alarm is generated.
 - If so, go to step 2.
 - If not, go to step 3.
 2. Handle the power alarm and check whether the alarm is cleared.
 - If the alarm is cleared, go to step 8.
 - If the alarm persists, go to step 3.
 3. Check the current of the board where the optical module resides and check whether a current alarm is generated on the NMS.
 - If so, go to step 4.
 - If not, go to step 5.
 4. Handle the current alarm and check whether the alarm is cleared.
 - If the alarm is cleared, go to step 8.
 - If the alarm persists, go to step 5.
 5. Replace the optical module and check whether the alarm is cleared.
 - If the alarm is cleared, go to step 8.
 - If the alarm persists, go to step 6.

6. Replace the board where the optical module resides and check whether the alarm is cleared.
 - If the alarm is cleared, go to step 8.
 - If the alarm persists, go to step 7.
 7. Collect alarm, log, and configuration information, and contact technical support engineers.
 8. End.
- Cause 16: The bias current of the optical module was too low.
 1. Run the display alarm all command to check whether the hwPowerInvalid alarm is generated.
 - If so, go to step 2.
 - If not, go to step 3.
 2. Handle the power alarm and check whether the alarm is cleared.
 - If the alarm is cleared, go to step 8.
 - If the alarm persists, go to step 3.
 3. Check the current of the board where the optical module resides and check whether a current alarm is generated on the NMS.
 - If so, go to step 4.
 - If not, go to step 5.
 4. Handle the current alarm and check whether the alarm is cleared.
 - If the alarm is cleared, go to step 8.
 - If the alarm persists, go to step 5.
 5. Replace the optical module and check whether the alarm is cleared.
 - If the alarm is cleared, go to step 8.
 - If the alarm persists, go to step 6.
 6. Replace the board where the optical module resides and check whether the alarm is cleared.
 - If the alarm is cleared, go to step 8.
 - If the alarm persists, go to step 7.
 7. Collect alarm, log, and configuration information, and contact technical support engineers.
 8. End.
 - Cause 17: The temperature of the optical module was too high.
 1. Run the display alarm all command to check whether the hwBoardInvalid alarm is generated.
 - If so, go to step 2.
 - If not, go to step 3.
 2. Handle the alarm and check whether the alarm is cleared.
 - If the alarm is cleared, go to step 8.
 - If the alarm persists, go to step 3.
 3. Check the temperature of the board where the optical module resides and check whether a board temperature alarm is generated on the NMS.

- If yes, go to step 4.
 - If no, go to step 5.
 - 4. Handle the board temperature alarm, and then check whether the alarm is cleared.
 - If the alarm is cleared, go to step 8.
 - If the alarm persists, go to step 5.
 - 5. Replace the optical module and check whether the alarm is cleared.
 - If the alarm is cleared, go to step 8.
 - If the alarm persists, go to step 6.
 - 6. Replace the board where the optical module resides and check whether the alarm is cleared.
 - If the alarm is cleared, go to step 8.
 - If the alarm persists, go to step 7.
 - 7. Collect alarm, log, and configuration information, and contact technical support engineers.
 - 8. End.
- Cause 18: The temperature of the optical module was too low.
 - 1. Run the display alarm all command to check whether a temperature alarm is generated.
 - If so, go to step 2.
 - If not, go to step 3.
 - 2. Handle the temperature alarm and check whether the alarm is cleared.
 - If the alarm is cleared, go to step 8.
 - If the alarm persists, go to step 3.
 - 3. Check the temperature of the board where the optical module resides and check whether a board temperature alarm is generated on the NMS.
 - If so, go to step 4.
 - If not, go to step 5.
 - 4. Handle the board temperature alarm, and then check whether the alarm is cleared.
 - If the alarm is cleared, go to step 8.
 - If the alarm persists, go to step 5.
 - 5. Replace the optical module and check whether the alarm is cleared.
 - If the alarm is cleared, go to step 8.
 - If the alarm persists, go to step 6.
 - 6. Replace the board where the optical module resides and check whether the alarm is cleared.
 - If the alarm is cleared, go to step 8.
 - If the alarm persists, go to step 7.
 - 7. Collect alarm, log, and configuration information, and contact technical support engineers.
 - 8. End.

- Cause 19: The power current of the optical module is too high.
 1. Run the display alarm all command to check whether the hwPowerInvalid alarm is generated.
 - If so, go to step 2.
 - If not, go to step 3.
 2. Handle the power alarm and check whether the alarm is cleared.
 - If the alarm is cleared, go to step 8.
 - If the alarm persists, go to step 3.
 3. Check the current of the board where the optical module resides and check whether a current alarm is generated on the NMS.
 - If so, go to step 4.
 - If not, go to step 5.
 4. Handle the current alarm and check whether the alarm is cleared.
 - If the alarm is cleared, go to step 8.
 - If the alarm persists, go to step 5.
 5. Replace the optical module and check whether the alarm is cleared.
 - If the alarm is cleared, go to step 8.
 - If the alarm persists, go to step 6.
 6. Replace the board where the optical module resides and check whether the alarm is cleared.
 - If the alarm is cleared, go to step 8.
 - If the alarm persists, go to step 7.
 7. Collect alarm, log, and configuration information, and contact technical support engineers.

Related Information

None.

3.5.1.16 ALM-135463100 hwIfMonitorCrcErrorRising

Description

The CRC error is rising. (hwIfMonitorIndex=[EntityPhysicalIndex], hwIfMonitorCrcErrorStatistics=[hwIfMonitorCrcErrorStatistics], hwIfMonitorCrcErrorThreshold=[hwIfMonitorCrcErrorThreshold], hwIfMonitorCrcErrorInterval=[hwIfMonitorCrcErrorInterval], EntPhysicalName=[EntPhysicalName], hwIfMonitorAllStatistics=[hwIfMonitorAllStatistics])

The number of CRC error packets received by the interface in a specified period exceeded the upper threshold.

Attribute

AlarmID	Alarm OID	Alarm Severity	Alarm Type
135463100	1.3.6.1.4.1.2011.5.25.41.4.1	Critical	Processing error alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
EntityPhysicalIndex	Entity index.
hwIfMonitorCrcErrorStatistics	Real-time statistics of CRC error packets
hwIfMonitorCrcErrorThreshold	Upper threshold for the number of CRC error packets
hwIfMonitorCrcErrorInterval	Configured statistics collection interval
EntPhysicalName	Entity name
hwIfMonitorAllStatistics	Number of packets in real-time statistics

Impact on the System

An interface receives a large number of CRC error packets, which may cause the interface to transit to the Error-Down state.

Possible Causes

The interface receives excessive CRC error packets whose lengths are greater than or equal to 64 bytes in a specified period of time.

Procedure

1. Run the **display this** command in the interface view to check whether the alarm threshold for error packets is too low. Determine the alarm threshold based on service requirements.

- If so, go to Step 2.
- If no, go to Step 3.

2. Run the **trap-threshold crc-statistics** command in the interface view to set a larger alarm threshold for error packets. Then check whether the alarm is cleared.

- If yes, no further action is required.

- If no, go to Step 3.
3. Collect trap, log, and configuration information, and contact technical support personnel.

Related Information

None.

3.5.1.17 ALM-15795006 hwPKILocalCertNearlyExpired

Description

PKI/4/PKILOCALCERTNEARLYEXPIRED: OID [*oid*] the local certificate is nearly expired. (LocalCertIssuer=[*issuer*], LocalCertSubject=[*subject*], LocalCertStartTime=[*starttime*], LocalCertFinishTime=[*finishtime*])

The local certificate is about to expire.

Attribute

Alarm ID	OID	Alarm Severity	Alarm Type
15795006	1.3.6.1.4.1.201 1.6.122.34.0.2. 14	Warning	Communication alarm

Parameters

Name	Meaning
oid	Indicates the MIB object ID of the alarm.
issuer	Indicates the issuer of the local certificate.
subject	Indicates the subject of the local certificate.
starttime	Indicates the start time of the local certificate.
finishtime	Indicates the end time of the local certificate.

Impact on the System

The service will be invalid after the certificate expires.

Possible Causes

The local certificate is about to expire. The local certificate expiration time is less than the certificate expired prewarning time configured by the **pki set-certificate expire-prewarning** command.

Procedure

- Step 1** Check whether the system time on the local device is correct.
- Step 2** If the system time is correct, apply for a new local certificate immediately.
- End

Clearing

The alarm needs to be cleared manually.

3.5.1.18 ALM-135462976 hwBoardRemove

Description

The board was removed. (EntPhysicalIndex=[EntPhysicalIndex], EntPhysicalName=[EntPhysicalName], EntityType=[EntityType], EntityTrapFaultID=[EntityTrapFaultID], Reason=[Reason])

A card is removed from the device.

Attribute

Alarm ID	OID	Alarm Severity	Alarm Type
135462976	1.3.6.1.4.1.2011.5.25.219.2.2.1	Warning	Equipment alarm

Parameters

Parameter	Description
EntPhysicalIndex	Entity index.
EntPhysicalName	Entity name.
EntityType	Entity type.
EntityTrapFaultID	Alarm cause.
Reason	

Impact on the System

All services on the board are interrupted, and the reliability of control data transmission between devices is affected.

Possible Causes

A board was removed.

Procedure

1. Check whether the board is removed manually.
 - If so, go to step 2.
 - If not, go to step 3.
2. Re-insert the board. After the board is started successfully, run the display device command to check whether the board is registered successfully.
 - If the registration is successful, the fault is rectified.
 - If the registration fails, go to step 3.
3. Collect alarm, log, and configuration information, and contact technical support personnel.

3.5.1.19 ALM-183312389 hwRadiusAuthServerDown

Description

The communication with the RADIUS authentication server fails.
(IpAddress=[IpAddress],Vpn-Instance=[Vpn-Instance])

The communication with the RADIUS authentication server fails.

Attribute

Alarm ID	OID	Alarm Severity	Alarm Type
183312389	1.3.6.1.4.1.2011.5 .25.40.15.2.2.1.2	Warning	Communication alarm

Parameters

Name	Meaning
IpAddress	Indicates the IP address of the RADIUS authentication server
Vpn-Instance	Indicates the VPN instance on the RADIUS authentication server

Impact on the System

The authentication fails and users cannot go online. If there is no backup server, online users may be forcibly logged out.

Possible Causes

The server did not respond to the request of the device within the timeout period.

Procedure

1. Run the **ping** command to check whether the RADIUS server is reachable.
 - If so, go to Step 3.
 - If not, go to Step 2.
2. Run the **display interface** command to check whether the interface is Up.
 - If so, go to Step 3.
 - If not, verify that the physical link is connected properly.
3. Run the **display current-configuration** command to check whether the RADIUS server is correctly configured.
 - If so, go to Step 4.
 - If not, modify configurations on the RADIUS server.
4. Collect the alarm information, log information, and configuration information, and then contact the Huawei technical support personnel.

3.5.1.20 ALM-183312391 hwRadiusAcctServerDown

Description

The communication with the RADIUS accounting server fails.
(IpAddress=[IpAddress],Vpn-Instance=[Vpn-Instance])

The communication with the RADIUS accounting server fails.

Attribute

Alarm ID	OID	Alarm Severity	Alarm Type
183312391	1.3.6.1.4.1.2011.5 .25.40.15.2.2.1.4	Warning	Communication alarm

Parameters

Name	Meaning
IpAddress	Indicates the IP address of the RADIUS accounting server

Name	Meaning
Vpn-Instance	Indicates the VPN instance on the RADIUS accounting server

Impact on the System

Accounting on online users may fail.

Possible Causes

The route between the device and the RADIUS accounting server was unreachable or the RADIUS accounting server did not respond to the request of the device within the timeout period.

Procedure

1. Run the **ping** command to check whether the RADIUS server is reachable.
 - If so, go to Step 3.
 - If not, go to Step 2.
2. Run the **display interface** command to check whether the interface is Up.
 - If so, go to Step 3.
 - If not, verify that the physical link is connected properly.
3. Run the **display current-configuration** command to check whether the RADIUS server is correctly configured.
 - If so, go to Step 4.
 - If not, modify configurations on the RADIUS server.
4. Collect the alarm information, log information, and configuration information, and then contact the Huawei technical support personnel.

3.5.1.21 ALM-135462996 hwBoardFail

Description

The board partially failed. (EntPhysicalIndex=[EntPhysicalIndex], EntPhysicalName=[EntPhysicalName], EntityType=[EntityType], EntityTrapFaultID=[EntityTrapFaultID], Reason=[Reason])

The card experienced a partial failure.

Attribute

AlarmID	Alarm OID	Alarm Severity	Alarm Type
135462996	1.3.6.1.4.1.2011.5.25.219.2.2.3	Critical	Equipment alarm

Parameters

Name	Meaning
EntPhysicalIndex	Entity index.
EntPhysicalName	Entity name.
EntityType	Entity type.
EntityTrapFaultID	Alarm cause.
Reason	

Impact on the System

- Cause 1: Power supply abnormal.
Services on the card may be affected or even interrupted.
- Cause 2: A voltage drop occurred on the board.
Services on the card may be affected or even interrupted.
- Cause 3: The serial management bus of the board malfunctions.
Services on the card may be affected or even interrupted.
- Cause 6: Board RTC fault.
Services on the card may be affected or even interrupted.
- Cause 8: The fan is not full.
As a result, fan information cannot be obtained.
- Cause 11: A data channel fault occurred on the forwarding engine.
Services on the card may be affected or even interrupted.
- Cause 12: The forwarding engine failed.
Services on the card may be affected or even interrupted.
- Cause 13: Inter-card broadcast traffic failed to be forwarded.
Services on the card may be affected or even interrupted.
- Cause 15: Fabric interface input or output bandwidth usage exceeded 90% continuously.
Services on the card may be affected or even interrupted.
- Cause 16: Ingress clock signals channel failed.
Services on the card may be affected or even interrupted.
- Cause 17: The sensor on the board was faulty.
Services on the card may be affected or even interrupted.
- Cause 18: Chip instability.
Services on the card may be affected or even interrupted.
- Cause 19: Egress clock signals channel failed.
Services on the card may be affected or even interrupted.
- Cause 20: A packet reassembly error occurred.
Services on the card may be affected or even interrupted.

- Cause 21: Board CANBUS failed.
Services on the card may be affected or even interrupted.
- Cause 23: Board cannot be powered on or powered off properly.
Services on the card may be affected or even interrupted.
- Cause 24: EEPROM is abnormal.
The current services are not affected, but the services after the next startup of the board are affected.
- Cause 25: The fan model does not match the device.
Services on the card may be affected or even interrupted.
- Cause 26: The power supply model does not match the device.
Services on the card may be affected or even interrupted.
- Cause 27: The PHY chip is abnormal.
Services on the card may be affected or even interrupted.
- Cause 29: Board PLL instability.
Services on the card may be affected or even interrupted.
- Cause 30: Phy instability.
Services on the card may be affected or even interrupted.
- Cause 36: USB overcurrent occurred.
Services on the card may be affected or even interrupted.
- Cause 37: IIC failed.
Services on the card may be affected or even interrupted.
- Cause 38: LANSWITCH chip instability.
Services on the card may be affected or even interrupted.
- Cause 39: The link of the XFI interface is faulty.
Services on the card may be affected or even interrupted.
- Cause 40: A CRC error occurred on the XFI interface.
Services on the card may be affected or even interrupted.
- Cause 43: The memory size is different from the standard configuration.
Services on the card may be affected or even interrupted.
- Cause 44: Flash memory failed.
Services on the card may be affected or even interrupted.
- Cause 50: CMU on the MPU is not registered.
Services on the card may be affected or even interrupted.
- Cause 51: The 38M clock fails.
Services on the card may be affected or even interrupted.
- Cause 52: The 19M clock fails.
Services on the card may be affected or even interrupted.
- Cause 53: The board clock fails.
Services on the card may be affected or even interrupted.
- Cause 54: The PLLA inside the forwarding engine is not ready.
Services on the card may be affected or even interrupted.

- Cause 55: The Serdes on the board failed.
Services on the card may be affected or even interrupted.
- Cause 56: An internal modular of the forwarding engine is abnormal.
Services on the card may be affected or even interrupted.
- Cause 58: The active and standby MPUs cannot communicate with each other.
Services on the card may be affected or even interrupted.
- Cause 59: The board type cannot be identified.
Services on the card may be affected or even interrupted.
- Cause 60: The board clock(156M) failed.
Services on the card may be affected or even interrupted.
- Cause 65: Storage media is abnormal.
Services on the card may be affected or even interrupted.
- Cause 70: CANBUS communications between the monitor chips failed.
Services on the card may be affected or even interrupted.
- Cause 71: A DDR fault occurs on the board.
Services on the card may be affected or even interrupted.
- Cause 72: The slot ID of the board fails to be checked.
Services on the card may be affected or even interrupted.
- Cause 73: Access to the flash memory of the board fails.
Services on the card may be affected or even interrupted.
- Cause 74: The FULLIN signal of the board is abnormal.
Services on the card may be affected or even interrupted.
- Cause 75: The slot ID signal from the CANBUS is abnormal.
Services on the card may be affected or even interrupted.
- Cause 76: A SerialCpldLocalbus fault occurs on the board.
Services on the card may be affected or even interrupted.
- Cause 77: The micro switch of the board fails.
Services on the card may be affected or even interrupted.
- Cause 78: The frequency synthesizer failed.
Services on the card may be affected or even interrupted.
- Cause 80: A CPU fault occurred.
Services on the card may be affected or even interrupted.
- Cause 82: A CPU-side CRC fault occurred.
Services on the card may be affected or even interrupted.
- Cause 83: A PHY-side CRC fault occurred.
Services on the card may be affected or even interrupted.
- Cause 84: The disk will soon become invalid.
Services on the card may be affected or even interrupted.
- Cause 88: The Chip is failed.
Services on the card may be affected or even interrupted.

- Cause 90: Overcurrent occurred on the board.
Services on the card may be affected or even interrupted.
- Cause 91: The FPGA is abnormal.
Services on the card may be affected or even interrupted.
- Cause 92: The sensor chip on the board was faulty.
Services on the card may be affected or even interrupted.
- Cause 96: A HTM chip fault occurred.
Services on the card may be affected or even interrupted.
- Cause 99: Failed to check the voltage of the board.
Services on the card may be affected or even interrupted.
- Cause 102: The currently used hard disk is not certified by Huawei.
Services on the card may be affected or even interrupted.
- Cause 103: The hard disk was pulled out.
Services on the card may be affected or even interrupted.
- Cause 104: The device certificate verification failed.
The key components of the board may have been replaced, which affects system reliability and security.
- Cause 105: Failed to access backplane IIC.
Services on the card may be affected or even interrupted.
- Cause 106: Failed to check backplane ID.
Services on the card may be affected or even interrupted.
- Cause 107: The IIC of MCU module is abnormal.
Services on the card may be affected or even interrupted.

Possible Causes

- Cause 1: Power supply abnormal.
- Cause 2: A voltage drop occurred on the board.
- Cause 3: The serial management bus of the board malfunctions.
- Cause 6: Board RTC fault.
- Cause 8: The fan is not full.
- Cause 11: A data channel fault occurred on the forwarding engine.
- Cause 12: The forwarding engine failed.
- Cause 13: Inter-card broadcast traffic failed to be forwarded.
- Cause 15: Fabric interface input or output bandwidth usage exceeded 90% continuously.
- Cause 16: Ingress clock signals channel failed.
- Cause 17: The sensor on the board was faulty.
- Cause 18: Chip instability.
- Cause 19: Egress clock signals channel failed.
- Cause 20: A packet reassembly error occurred.
- Cause 21: Board CANBUS failed.

- Cause 23: Board cannot be powered on or powered off properly.
- Cause 24: EEPROM is abnormal.
- Cause 25: The fan model does not match the device.
- Cause 26: The power supply model does not match the device.
- Cause 27: The PHY chip is abnormal.
- Cause 29: Board PLL instability.
- Cause 30: Phy instability.
- Cause 36: USB overcurrent occurred.
- Cause 37: IIC failed.
- Cause 38: LANSWITCH chip instability.
- Cause 39: The link of the XFI interface is faulty.
- Cause 40: A CRC error occurred on the XFI interface.
- Cause 43: The memory size is different from the standard configuration.
- Cause 44: Flash memory failed.
- Cause 50: CMU on the MPU is not registered.
- Cause 51: The 38M clock fails.
- Cause 52: The 19M clock fails.
- Cause 53: The board clock fails.
- Cause 54: The PLLA inside the forwarding engine is not ready.
- Cause 55: The Serdes on the board failed.
- Cause 56: An internal modular of the forwarding engine is abnormal.
- Cause 58: The active and standby MPUs cannot communicate with each other.
- Cause 59: The board type cannot be identified.
- Cause 60: The board clock(156M) failed.
- Cause 65: Storage media is abnormal.
- Cause 70: CANBUS communications between the monitor chips failed.
- Cause 71: A DDR fault occurs on the board.
- Cause 72: The slot ID of the board fails to be checked.
- Cause 73: Access to the flash memory of the board fails.
- Cause 74: The FULLIN signal of the board is abnormal.
- Cause 75: The slot ID signal from the CANBUS is abnormal.
- Cause 76: A SerialCpldLocalbus fault occurs on the board.
- Cause 77: The micro switch of the board fails.
- Cause 78: The frequency synthesizer failed.
- Cause 80: A CPU fault occurred.
- Cause 82: A CPU-side CRC fault occurred.
- Cause 83: A PHY-side CRC fault occurred.
- Cause 84: The disk will soon become invalid.
- Cause 88: The Chip is failed.
- Cause 90: Overcurrent occurred on the board.

- Cause 91: The FPGA is abnormal.
- Cause 92: The sensor chip on the board was faulty.
- Cause 96: A HTM chip fault occurred.
- Cause 99: Failed to check the voltage of the board.
- Cause 102: The currently used hard disk is not certified by Huawei.
- Cause 103: The hard disk was pulled out.
- Cause 104: The device certificate verification failed.
- Cause 105: Failed to access backplane IIC.
- Cause 106: Failed to check backplane ID.
- Cause 107: The IIC of MCU module is abnormal.

Procedure

- Cause 1: Power supply abnormal.
 1. If the faulty board is not reset or powered off and services are running properly, go to step 3.
 2. Power off and then power on the faulty board. If the fault persists, go to step 3.
 3. Collect trap, log, and configuration information, and contact technical support personnel.
- Cause 2: A voltage drop occurred on the board.
 1. Collect alarm, log, and configuration information, and contact technical support personnel.
- Cause 3: The serial management bus of the board malfunctions.
 1. Collect alarm, log, and configuration information, and contact technical support personnel.
- Cause 6: Board RTC fault.
 1. If the faulty board is not reset or powered off and services are running properly, go to step 3.
 2. Power off and then power on the faulty board. If the fault persists, go to step 3.
 3. Collect trap, log, and configuration information, and contact technical support personnel.
- Cause 8: The fan is not full.

Insert the fan module into the corresponding slot.
- Cause 11: A data channel fault occurred on the forwarding engine.
 1. Reset the board. If the fault persists, go to step 2.
 2. Collect trap, log, and configuration information, and contact technical support personnel.
- Cause 12: The forwarding engine failed.
 1. Reset the board. If the fault persists, go to step 2.
 2. Collect trap, log, and configuration information, and contact technical support personnel.
- Cause 13: Inter-card broadcast traffic failed to be forwarded.

1. Collect alarm and log information, and contact technical support personnel.
- Cause 15: Fabric interface input or output bandwidth usage exceeded 90% continuously.
 1. Collect alarm and log information, and contact technical support personnel.
- Cause 16: Ingress clock signals channel failed.
 1. Collect alarm and log information, and contact technical support personnel.
- Cause 17: The sensor on the board was faulty.
 1. Reset the board. If the fault persists, go to step 2.
 2. Collect trap, log, and configuration information, and contact technical support personnel.
- Cause 18: Chip instability.
 1. Reset the board. If the fault persists, go to step 2.
 2. Collect trap, log, and configuration information, and contact technical support personnel.
- Cause 19: Egress clock signals channel failed.
 1. Collect alarm and log information, and contact technical support personnel.
- Cause 20: A packet reassembly error occurred.
 1. Collect alarm and log information, and contact technical support personnel.
- Cause 21: Board CANBUS failed.
 1. Reset the faulty board. If the fault persists, go to step 2.
 2. Collect trap, log, and configuration information, and contact technical support personnel.
- Cause 23: Board cannot be powered on or powered off properly.
 1. Power off and then power on the faulty board. If the fault persists, go to step 2.
 2. Collect trap, log, and configuration information, and contact technical support personnel.
- Cause 24: EEPROM is abnormal.
 1. Check whether the services on the board are normal.
 - If so, go to step 4.
 - If not, go to step 2.
 2. Securely insert the board, and then check whether the alarm is cleared.
 - If so, go to step 5.
 - If not, go to step 3.
 3. Replace the faulty board, and then check whether the alarm is cleared.
 - If so, go to step 5.
 - If not, go to step 4.
 4. Collect alarm, log, and configuration information, and contact technical support engineers.
 5. End.
- Cause 25: The fan model does not match the device.
 1. Replace the fan module with one that matches the device model.

- Cause 26: The power supply model does not match the device.
 1. Replace the fan or power module with a new one that matches the device model.
- Cause 27: The PHY chip is abnormal.
 1. Collect alarm, log, and configuration information, and contact technical support personnel.
- Cause 29: Board PLL instability.
 1. Reset and restart the system.
 2. If the fault persists, replace the board.
- Cause 30: Phy instability.
 1. If the faulty board is not reset or powered off and services are running properly, go to step 3.
 2. Power off and then power on the faulty board. If the fault persists, go to step 3.
 3. Collect trap, log, and configuration information, and contact technical support personnel.
- Cause 36: USB overcurrent occurred.
 1. Collect alarm, log, and configuration information, and contact technical support personnel.
- Cause 37: IIC failed.
 1. Collect alarm, log, and configuration information, and contact technical support personnel.
- Cause 38: LANSWITCH chip instability.
 1. Reset the board. If the fault persists, go to step 2.
 2. Collect trap, log, and configuration information, and contact technical support personnel.
- Cause 39: The link of the XFI interface is faulty.
 1. Collect alarm, log, and configuration information, and contact technical support personnel.
- Cause 40: A CRC error occurred on the XFI interface.
 1. Collect alarm, log, and configuration information, and contact technical support personnel.
- Cause 43: The memory size is different from the standard configuration.
 1. Run the display version command to check whether the board memory meets the specifications. If the board memory does not meet the specifications, contact technical support personnel.
- Cause 44: Flash memory failed.
 1. Reset the board. If the fault persists, go to step 2.
 2. Collect trap, log, and configuration information, and contact technical support personnel.
- Cause 50: CMU on the MPU is not registered.

Collect alarm, log, and configuration information and contact Huawei technical support.
- Cause 51: The 38M clock fails.

1. Collect alarm, log, and configuration information, and contact technical support personnel.
- Cause 52: The 19M clock fails.
Collect alarm, log, and configuration information and contact Huawei technical support.
- Cause 53: The board clock fails.
1. Collect alarm, log, and configuration information, and contact technical support personnel.
- Cause 54: The PLLA inside the forwarding engine is not ready.
1. Collect alarm, log, and configuration information, and contact technical support personnel.
- Cause 55: The Serdes on the board failed.
1. Reset the board. If the fault persists, go to step 2.
2. Collect trap, log, and configuration information, and contact technical support personnel.
- Cause 56: An internal modular of the forwarding engine is abnormal.
1. Collect alarm, log, and configuration information, and contact technical support personnel.
- Cause 58: The active and standby MPUs cannot communicate with each other.
1. Collect alarm, log, and configuration information, and contact technical support personnel.
- Cause 59: The board type cannot be identified.
1. Collect alarm and log information, and contact technical support personnel.
- Cause 60: The board clock(156M) failed.
Collect alarm and log information and contact Huawei technical support.
- Cause 65: Storage media is abnormal.
1. Collect alarm, log, and configuration information, and contact technical support personnel.
- Cause 70: CANBUS communications between the monitor chips failed.
1. Collect alarm, log, and configuration information, and contact technical support personnel.
- Cause 71: A DDR fault occurs on the board.
1. Collect alarm, log, and configuration information, and contact technical support personnel.
- Cause 72: The slot ID of the board fails to be checked.
1. Collect alarm, log, and configuration information, and contact technical support personnel.
- Cause 73: Access to the flash memory of the board fails.
1. Collect alarm, log, and configuration information, and contact technical support personnel.
- Cause 74: The FULLIN signal of the board is abnormal.
1. Collect alarm, log, and configuration information, and contact technical support personnel.

- Cause 75: The slot ID signal from the CANBUS is abnormal.
1. Collect alarm, log, and configuration information, and contact technical support personnel.
- Cause 76: A SerialCpldLocalbus fault occurs on the board.
1. Collect alarm, log, and configuration information, and contact technical support personnel.
- Cause 77: The micro switch of the board fails.
1. Collect alarm, log, and configuration information, and contact technical support personnel.
- Cause 78: The frequency synthesizer failed.
1. Collect alarm, log, and configuration information, and contact technical support personnel.
- Cause 80: A CPU fault occurred.
1. Collect alarm, log, and configuration information, and contact technical support personnel.
- Cause 82: A CPU-side CRC fault occurred.
1. Collect alarm, log, and configuration information, and contact technical support personnel.
- Cause 83: A PHY-side CRC fault occurred.
1. Collect alarm, log, and configuration information, and contact technical support personnel.
- Cause 84: The disk will soon become invalid.
1. Collect alarm, log, and configuration information, and contact technical support personnel.
- Cause 88: The Chip is failed.
1. Collect alarm, log, and configuration information, and contact technical support personnel.
- Cause 90: Overcurrent occurred on the board.
1. Collect alarm, log, and configuration information, and contact technical support personnel.
- Cause 91: The FPGA is abnormal.
1. Collect alarm, log, and configuration information, and contact technical support personnel.
- Cause 92: The sensor chip on the board was faulty.
1. Collect alarm, log, and configuration information, and contact technical support personnel.
- Cause 96: A HTM chip fault occurred.
1. Collect alarm, log, and configuration information, and contact technical support personnel.
- Cause 99: Failed to check the voltage of the board.
1. Collect alarm, log, and configuration information, and contact technical support personnel.
- Cause 102: The currently used hard disk is not certified by Huawei.
Remove non-Huawei-certified hard disks and insert Huawei-certified hard disks.

- Cause 103: The hard disk was pulled out.
Insert a hard disk.
- Cause 104: The device certificate verification failed.
Reset the board and check whether the fault is rectified. If the fault persists, replace the board.
- Cause 105: Failed to access backplane IIC.
Collect alarm, log, and configuration information and contact Huawei technical support.
- Cause 106: Failed to check backplane ID.
Collect alarm, log, and configuration information and contact Huawei technical support.
- Cause 107: The IIC of MCU module is abnormal.
Collect alarm, log, and configuration information and contact Huawei technical support.

Related Information

None.

3.5.1.22 ALM-15795011 hwPKICACertInvalid

Description

PKI/2/PKICACERTINVALID: OID [*oid*] the CA certificate is invalid.
(CACertIssuer=[*issuer*], CACertSubject=[*subject*], CACertStartTime=[*starttime*], CACertFinishTime=[*finishtime*])

The CA certificate is invalid.

Attribute

Alarm ID	OID	Alarm Severity	Alarm Type
15795011	1.3.6.1.4.1.201 1.6.122.34.0.2. 9	Major	Communication alarm

Parameters

Name	Meaning
oid	Indicates the MIB object ID of the alarm.
issuer	Indicates the issuer of the CA certificate.

Name	Meaning
subject	Indicates the subject of the CA certificate.
starttime	Indicates the start time of the CA certificate.
finishtime	Indicates the end time of the CA certificate.

Impact on the System

The service becomes invalid.

Possible Causes

The CA certificate is invalid.

Procedure

Step 1 Run the **display clock** command to check whether the device time is correct.If not, run the **clock datetime** command in the user view to change the device time.

Step 2 Apply for a new certificate through SCEP or CMPv2 online or apply for a new certificate offline. For details, see the *Huawei AR SeriesV300R021 Configuration Guide - PKI Configuration*.

----End

Clearing

The alarm needs to be cleared manually.

3.5.1.23 ALM-15795010 hwPKICACertNearlyExpired

Description

PKI/4/PKICACERTNEARLYEXPIRED: OID [*oid*] the CA certificate is nearly expired. (CACertIssuer=[*issuer*], CACertSubject=[*subject*], CACertStartTime=[*starttime*], CACertFinishTime=[*finishtime*])

The CA certificate is about to expire.

Attribute

Alarm ID	OID	Alarm Severity	Alarm Type
15795010	1.3.6.1.4.1.2011.6.122.34.0.2.11	Warning	Communication alarm

Parameters

Name	Meaning
<i>oid</i>	Indicates the MIB object ID of the alarm.
<i>issuer</i>	Indicates the issuer of the CA certificate.
<i>subject</i>	Indicates the subject of the CA certificate.
<i>starttime</i>	Indicates the start time of the CA certificate.
<i>finishtime</i>	Indicates the end time of the CA certificate.

Impact on the System

The service will be invalid after the certificate expires.

Possible Causes

The CA certificate is about to expire. The CA certificate expiration time is less than the certificate expired prewarning time configured by the **pki set-certificate expire-prewarning** command.

Procedure

- Step 1** Run the **display clock** command to check whether the device time is correct. If not, run the **clock datetime** command in the user view to change the device time.
- Step 2** Apply for a new certificate through SCEP or CMPv2 online or apply for a new certificate offline. For details, see the *Huawei AR Series V300R021 Configuration Guide - PKI Configuration*
- End

Clearing

The alarm needs to be cleared manually.

3.5.1.24 ALM-15795009 hwPKICrlInvalid

Description

PKI/2/PKICRLINVALID: OID [*oid*] the crl is invalid. (CrlIssuer=[*crlissuer*], CrlStartTime=[*crlstarttime*], CrlFinishTime=[*crlfinishtime*])

The CRL is invalid.

Attribute

Alarm ID	OID	Alarm Severity	Alarm Type
15795009	1.3.6.1.4.1.201 1.6.122.34.0.2. 15	Major	Communication alarm

Parameters

Name	Meaning
oid	Indicates the MIB object ID of the alarm.
crlissuer	Indicates the issuer of the CRL.
crlstarttime	Indicates the start time of the CRL.
crlfinishtime	Indicates the end time of the CRL.

Impact on the System

The service becomes invalid.

Possible Causes

Indicates that the current system time is out of the CRL validity period.

Procedure

- Step 1** Run the **display clock** command to check whether the device time is correct.If not, run the **clock datetime** command in the user view to change the device time.
- Step 2** Obtain a new CRL. For details, see "Configuring Local Certificate Check" in *Huawei AR SeriesV300R021 Configuration Guide - PKI Configuration*.
- End

Clearing

The alarm needs to be cleared manually.

3.5.1.25 ALM-15795008 hwPKICrINearlyExpired

Description

PKI/4/PKICRLNEARLYEXPIRED: OID [*oid*] the crl is nearly expired.
(CrlIssuer=[*crlissuer*], CrlStartTime=[*crlstarttime*], CrlFinishTime=[*crlfinishtime*])
The CRL is about to expire

Attribute

Alarm ID	OID	Alarm Severity	Alarm Type
15795008	1.3.6.1.4.1.201 1.6.122.34.0.2. 17	Warning	Communication alarm

Parameters

Name	Meaning
oid	Indicates the MIB object ID of the alarm.
crlissuer	Indicates the issuer of the CRL.
crlstarttime	Indicates the start time of the CRL.
crlfinishtime	Indicates the end time of the CRL.

Impact on the System

The service becomes invalid.

Possible Causes

The CRL is to expire. The CRL expiration time is less than 2 hours ahead of the current system time.

Procedure

Step 1 Run the **display clock** command to check whether the device time is correct.If not, run the **clock datetime** command in the user view to change the device time.

Step 2 Obtain a new CRL. For details, see "Configuring Local Certificate Check" in *Huawei AR SeriesV300R021 Configuration Guide - PKI Configuration*.

----End

Clearing

The alarm needs to be cleared manually.

3.5.1.26 ALM-15795049 hwHrpDeviceID

Description

HRP link changes to [hwHrpTrapLinkState]. Local device ID is [hwHrpTrapLocalID], peer device ID is [hwHrpTrapPeerID].

The heartbeat status of the high availability system is abnormal.

Attribute

Alarm ID	OID	Alarm Severity	Alarm Type
15795049	1.3.6.1.4.1.2011.6.122.51.2.2.2	Critical	Quality of service alarm

Parameters

Name	Meaning
hwHrpTrapLinkState	Connection status of dual-system hot backup
hwHrpTrapLocalID	MAC address of the management network port on the local device
hwHrpTrapPeerID	MAC address of the management network port on the remote device.

Impact on the System

If both the active and standby devices are in the active state, services are interrupted.

Possible Causes

- Cause 1: Manually disable dual hot standby function.
- Cause 2: The link between the heartbeat interfaces of the active and standby devices is interrupted.
- Cause 3: The master device or the backup device fails to send and receive heartbeat packets.

Procedure

- Cause 1: Manually disable dual hot standby function.
Check whether the hot standby configuration on the active and standby devices is correct.
- Cause 2: The link between the heartbeat interfaces of the active and standby devices is interrupted.
Run the ping command to check whether the link between the heartbeat interfaces of the active and standby devices is normal.
- Cause 3: The master device or the backup device fails to send and receive heartbeat packets.
Check whether the status of the active and standby devices is normal.

Clearing

After the fault is rectified, the system clears this alarm, removing the need to manually clear it. This alarm will not be displayed on the **CurrentAlarms** page.

3.5.1.27 ALM-135462941 hwPowerFail

Description

A power module experienced a partial failure.
(EntPhysicalIndex=[EntPhysicalIndex], EntPhysicalName=[EntPhysicalName], EntityTrapFaultID=[EntityTrapFaultID], EntityOperStatus=[EntityOperStatus], Reason=[ReasonDsp])

A power module experienced a partial failure.

Attribute

AlarmID	Alarm OID	Alarm Severity	Alarm Type
135462941	1.3.6.1.4.1.2011.5.25 .219.2.5.3	Major	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
EntPhysicalIndex	Entity index.
EntPhysicalName	Entity name.
EntityTrapFaultID	Fault ID.
EntityOperStatus	Alarm status information.
ReasonDsp	Alarm cause.

Impact on the System

- Cause 1: Communication failed between power and MPU.
If the power supply of the power module is abnormal, the power supply of the device may be insufficient. As a result, the board may be reset, which indirectly affects services and needs to be handled.
- Cause 2: Airflow direction is abnormal.
If the power supply of the power module is abnormal, the power supply of the device may be insufficient. As a result, the board may be reset, which indirectly affects services and needs to be handled.

- Cause 3: The fan inside a power module fails.
If the power supply of the power module is abnormal, the power supply of the device may be insufficient. As a result, the board may be reset, which indirectly affects services and needs to be handled.
- Cause 4: The power supply switch failed.
If the power supply of the power module is abnormal, the power supply of the device may be insufficient. As a result, the board may be reset, which indirectly affects services and needs to be handled.
- Cause 5: The current slight share.
If the power supply of the power module is abnormal, the power supply of the device may be insufficient. As a result, the board may be reset, which indirectly affects services and needs to be handled.
- Cause 6: The power module runs an earlier version.
If the power supply of the power module is abnormal, the power supply of the device may be insufficient. As a result, the board may be reset, which indirectly affects services and needs to be handled.
- Cause 7: Power Partial Failure.
If the power supply of the power module is abnormal, the power supply of the device may be insufficient. As a result, the board may be reset, which indirectly affects services and needs to be handled.
- Cause 8: The power module was present but the output was abnormal.
If the power supply of the power module is abnormal, the power supply of the device may be insufficient. As a result, the board may be reset, which indirectly affects services and needs to be handled.
- Cause 9: Two CAN bus connections were abnormal, and communication with the power module was interrupted.
If the power supply of the power module is abnormal, the power supply of the device may be insufficient. As a result, the board may be reset, which indirectly affects services and needs to be handled.
- Cause 10: The fan module in the power module run at full speed.
Services are not affected.
- Cause 11: The EEPROM module in a power module was faulty.
The power module is working properly, but the power data cannot be read.
- Cause 12: The power module is protected and cannot work properly.
If the power supply of the power module is abnormal, the power supply of the device may be insufficient. As a result, the board may be reset, which indirectly affects services and needs to be handled.
- Cause 13: The power id address conflict.
If the power supply of the power module is abnormal, the power supply of the device may be insufficient. As a result, the board may be reset, which indirectly affects services and needs to be handled.
- Cause 14: The current of the power is not average.
The power supply fault may cause insufficient power supply for the device and reset of the board, which indirectly affects services. Therefore, the fault must be rectified immediately.

- Cause 15: The current exceed the max value.
Services are affected.

Possible Causes

- Cause 1: Communication failed between power and MPU.
- Cause 2: Airflow direction is abnormal.
- Cause 3: The fan inside a power module fails.
- Cause 4: The power supply switch failed.
- Cause 5: The current slight share.
- Cause 6: The power module runs an earlier version.
- Cause 7: Power Partial Failure.
- Cause 8: The power module was present but the output was abnormal.
- Cause 9: Two CAN bus connections were abnormal, and communication with the power module was interrupted.
- Cause 10: The fan module in the power module run at full speed.
- Cause 11: The EEPROM module in a power module was faulty.
- Cause 12: The power module is protected and cannot work properly.
- Cause 13: The power id address conflict.
- Cause 14: The current of the power is not average.
- Cause 15: The current exceed the max value.

Procedure

- Cause 1: Communication failed between power and MPU.
 - a. Remove and reinstall the power module. If the fault persists, go to step 2.
 - b. Replace the power module. If the fault persists, go to step 3.
 - c. Collect trap, log, and configuration information, and contact technical support personnel.
- Cause 2: Airflow direction is abnormal.
 - a. Replace the power module. If the fault persists, collect trap, log, and configuration information, and contact technical support personnel.
- Cause 3: The fan inside a power module fails.
 - a. Power off the faulty power module and replace it.
- Cause 4: The power supply switch failed.
 - a. Manually turn on the power switch on the backplane.
- Cause 5: The current slight share.
 - a. Reduce the length of the network cable to reduce the power consumption of the board.If the fault persists, go to step 2.
 - b. If other power supplies are not powered on, power on them.If the fault persists, go to Step 3.
 - c. Replace the power module.
- Cause 6: The power module runs an earlier version.

- a. Run the upgrade power command in the diagnostic view to upgrade the power module.
- Cause 7: Power Partial Failure.
 - a. Collect trap, log, and configuration information, and contact technical support personnel.
- Cause 8: The power module was present but the output was abnormal.
 - 1. Collect trap, log, and configuration information, and contact technical support personnel.
- Cause 9: Two CAN bus connections were abnormal, and communication with the power module was interrupted.
 - 1. Collect trap, log, and configuration information, and contact technical support personnel.
- Cause 10: The fan module in the power module run at full speed.
 - 1. Lower the device temperature. After the temperature of the power module decreases, the fan speed automatically decreases.
- Cause 11: The EEPROM module in a power module was faulty.
 - 1. Collect trap, log, and configuration information, and contact technical support personnel.
- Cause 12: The power module is protected and cannot work properly.
 - 1. Collect trap, log, and configuration information, and contact technical support personnel.
- Cause 13: The power id address conflict.
 - 1. Power off the faulty power module and replace it.
 - 2. If the alarm persists, collect alarm, log, and configuration information, and contact technical support personnel.
- Cause 14: The current of the power is not average.
 - 1. If the faulty PM module is newly inserted, check whether it is properly inserted, the backplane has bent pins, or its connector is faulty.
 - If so, go to step 2.
 - If not, go to step 3.
 - 2. Perform the following operations according to the actual situation:
 - If the PM module is not securely installed, install it properly.
 - If the backplane has bent pins, do not insert the new PM into the faulty slot and contact Huawei technical support personnel.
 - If only the PM module connector is faulty, replace the PM module.
 - If the PM module is not newly inserted, go to step 3.
 - 3. Collect alarm, log, and configuration information, and contact technical support engineers.
- Cause 15: The current exceed the max value.
 - 1. Check whether the PM module is properly installed.
 - If so, go to step 3.
 - If not, go to step 2.
 - 2. Securely insert the faulty PM and check whether the alarm is cleared.

- If so, go to step 7.
- If not, go to step 3.
- 3. Check whether there are bent pins.
- If so, go to step 6.
- If not, go to step 4.
- 4. Check whether the PM connector is faulty.
- If so, go to step 5.
- If not, go to step 6.
- 5. Replace the PM and check whether the alarm is cleared.
- If so, go to step 7.
- If not, go to step 4.
- 6. Collect trap, log, and configuration information, and contact technical support personnel.
- 7. The procedure ends.

Related Information

None.

3.5.1.28 ALM-135462923 hwBrdTempFatalAlarm

Description

The board temperature exceeded the fatal alarm threshold.
(EntPhysicalIndex=[EntPhysicalIndex], EntPhysicalName=[EntPhysicalName], EntityThresholdType=[EntityThresholdType], EntityThresholdCritical=[EntityThresholdCritical], EntityThresholdCurrent=[EntityThresholdCurrent], EntityTrapFaultID=[EntityTrapFaultID],Reason=[ReasonDsp])

A major alarm was generated for the board or subcard temperature.

Attribute

AlarmID	Alarm OID	Alarm Severity	Alarm Type
135462923	1.3.6.1.4.1.2011.5.25.219.2.10.15	Critical	Environmental alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
EntPhysicalIndex	Entity index.

Name	Meaning
EntPhysicalName	Entity Name
EntityThresholdType	Entity Threshold Type
EntityThresholdCritical	Entity temperature threshold
EntityThresholdCurrent	Current temperature.
EntityTrapFaultID	Fault Code
ReasonDsp	Alarm cause

Impact on the System

- Cause 1: The board temperature was extremely high.
The temperature of the board is too high, which may cause the board to reset.
The temperature of the board is too high, which may cause the board to be powered off.
- Cause 2: The card temperature was extremely high.
The subcard temperature is too high, which may cause the board to reset.

Possible Causes

- Cause 1: The board temperature was extremely high.
- Cause 2: The card temperature was extremely high.

Procedure

- Cause 1: The board temperature was extremely high.
 1. Check whether the air filter of the fan is blocked.
 - If yes, clean the air filter.
 - If not, go to step 2.
 2. Check whether the temperature in the environment is excessively high.
 - If yes, lower the ambient temperature.
 - If not, go to step 3.
 3. Check whether the fan is faulty.
 - If yes, rectify the fan fault.
 - If no, go to Step 4.
 4. Check whether filler panels are installed in vacant slots.
 - If yes, go to step 5.
 - If not, insert a filler panel.
 5. Collect alarm, log, and configuration information and contact technical support personnel.
- Cause 2: The card temperature was extremely high.

1. Check whether the air filter of the fan is blocked.
 - If yes, clean the air filter.
 - If not, go to step 2.
2. Check whether the temperature in the environment is excessively high.
 - If yes, lower the ambient temperature.
 - If not, go to step 3.
3. Check whether the fan is faulty.
 - If yes, rectify the fan fault.
 - If no, go to Step 4.
4. Check whether a filler panel is installed in the vacant slot.
 - If yes, go to step 5.
 - If not, insert a filler panel.
5. Collect alarm, log, and configuration information and contact technical support personnel.

Related Information

None.

3.5.1.29 ALM-157024261 hwGtlNearDeadline

Description

License is near deadline, remaining [hwGtlRemainTime] day (s). Apply for a new license file from Huawei before the grace period expires. Otherwise, relevant service functions may be unavailable or the configuration may become ineffective. (FeatureName=[hwGtlFeatureName], ChassisIDorSlotID=[hwGtlChassisID]).

The license file is about to expire. Apply for a new license file from Huawei before the grace period expires. Otherwise, related service functions may be unavailable or the configuration may become invalid.

Attribute

AlarmID	Alarm OID	Alarm Severity	Alarm Type
157024261	1.3.6.1.4.1.2011.5.25 .142.2.3	Critical	Quality of service alarm

Parameters

Name	Meaning
hwGtlRemainTime	Time when the feature can remain in the grace period.

Name	Meaning
hwGtlFeatureName	Name of the feature in the grace period.
hwGtlChassisID	Description of a subrack or board.
hwGtlNearDeadlineReason	Reason why the license enters the grace period.

Impact on the System

Services are not affected.

Possible Causes

- License file expires.
- License file has been revoked.
- ESN mismatches.
- The specified license feature expires.

Procedure

Apply for a new license file from Huawei before the grace period expires.

Related Information

None.

3.5.1.30 ALM-157024262 hwGtlDefaultValue

Description

Current license value is default, the reason is [hwGtlDefaultValueReason].
(SlotID=[hwGtlChassisID])

The license file has expired.

Attribute

AlarmID	Alarm OID	Alarm Severity	Alarm Type
157024262	1.3.6.1.4.1.2011.5.25 .142.2.1	Critical	Quality of service alarm

Parameters

Name	Meaning
hwGtlFeatureName	Name of a feature.
hwGtlDefaultValueReason	Reason why the license expires.
hwGtlChassisID	ID of the chassis to which the license file belongs
hwGtlExpiredDay	Number of days that the license has expired.

Impact on the System

- Cause 0: License file expires.
After the license file is expired, all default control items activated by the license are restored to default values.
- Cause 1: License file has been revoked.
After the license file is expired, all default control items activated by the license are restored to default values.
- Cause 2: ESN mismatches.
After the license file is expired, all default control items activated by the license are restored to default values.
- Cause 4: The specified license feature expires.
After the license feature expires, the control items of the license feature are restored to the default values.

Possible Causes

- Cause 0: License file expires.
- Cause 1: License file has been revoked.
- Cause 2: ESN mismatches.
- Cause 4: The specified license feature expires.

Procedure

- Apply for a new valid license from Huawei.

Related Information

None.

3.5.1.31 ALM-135463092 hwChassisFail

Description

The chassis partially failed. (EntPhysicalIndex=[EntPhysicalIndex], EntPhysicalName=[EntPhysicalName], EntityTrapFaultID=[EntityTrapFaultID], Reason=[Reason])

A chassis experienced a partial failure.

Attribute

AlarmID	Alarm OID	Alarm Severity	Alarm Type
135463092	1.3.6.1.4.1.2011.5.25.219.2.1.3	Critical	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
EntPhysicalIndex	Index of a physical entity.
EntPhysicalName	Entity name.
EntityTrapFaultID	Alarm cause.
Reason	

Impact on the System

The system may become abnormal.

Possible Causes

- Cause 1: Different SFUs were installed in the same chassis.
- Cause 2: The system power or the power of the backup power supply is insufficient.
- Cause 3: No SFU is present in the chassis.
- Cause 4: No LPU is present in the chassis.
- Cause 5: No CMU is present in the chassis.
- Cause 6: The power module types are inconsistent.
- Cause 7: Failed to obtain slot information of the power supply.
- Cause 8: There is two or more fans not detected.
- Cause 9: The number of detected SFUs does not meet requirements.

Procedure

- Cause 1: Different SFUs were installed in the same chassis.
1. Insert the correct SFU.
- Cause 2: The system power or the power of the backup power supply is insufficient.
1. Add a power module.
- Cause 3: No SFU is present in the chassis.
1. Insert the SFU.
- Cause 4: No LPU is present in the chassis.
1. Insert the LPU.
- Cause 5: No CMU is present in the chassis.
1. Insert the CMU.
- Cause 6: The power module types are inconsistent.
1. Install only DC or AC power modules into all the power slots on the device.
- Cause 7: Failed to obtain slot information of the power supply.
1. Insert the power module into another slot. If the alarm persists, replace the power module.
- Cause 8: There is two or more fans not detected.
1. Install all the fan modules.
- Cause 9: The number of detected SFUs does not meet requirements.
1. Insert the SFU.

Related Information

None.

3.5.2 AR Alarms

3.5.2.1 ALM-142147599 bgpBackwardTransition

Description

The BGP FSM moves from a higher numbered state to a lower numbered state. (BgpPeerRemoteAddr=[PeerIpv4|pv6Addr], BgpPeerLastError=[PeerLastError], BgpPeerState=[PeerState], LocalIfName=[LocalIfName], Reason=[Reason])

The BGP FSM moved from a higher numbered state, namely, Openconfirm or Established, to a lower numbered state.

Attribute

Alarm ID	OID	Alarm Severity	Alarm Type
142147599	1.3.6.1.2.1.15.7.2	Major	Communication alarm

Parameters

Name	Meaning
PeerIpv4Ipv6Addr	Peer address.
PeerLastError	Error code returned when the peer was disconnected last time. The value of this parameter is displayed in the format of [ErrorCode] [ErrorSubCode], where [ErrorCode] indicates an error code and [ErrorSubCode] indicates an error subcode. For example, in the value 35, 3 indicates an error code and 5 indicates an error subcode. The value 0 indicates that no error occurs. For the meanings and possible causes of error codes, see BGP Principles - BGP Notification Packets. These packets are used to process various errors in the BGP process.
PeerState	Status of the BGP peer relationship.
LocalIfName	Local interface name.
Reason	Reason why the peer relationship is interrupted. • Configuration lead peer down: The configuration causes the peer disconnection. • Receive notification: Notification packets are received. • Receive error packet: Error packets are received. • Hold timer expire: The Hold timer expires. • Remote peer not reachable: The remote peer is unreachable. • Direct connect-interface down: The directly connected interface is Down. • Route limit: The number of routes exceeds the upper limit.

Impact on the System

The BGP peer relationship is interrupted, the route from the local device to the remote device is unreachable, and BGP forwarding services are interrupted.

Possible Causes

- Cause 1: BGP configuration lead peer down
- Cause 2: BGP receive notification
- Cause 3: BGP receive error packet
- Cause 4: BGP hold timer expire
- Cause 5: BGP remote peer not reachable
- Cause 6: BGP direct connect-interface down
- Cause 7: BGP route exceed the maximum number allowed

Procedure

- Cause 1: BGP configuration lead peer down
 1. Check whether the BGP peer relationship is interrupted because of the improper configurations of the local device.
 - If the configurations of the local device are improper, go to Step 2.
 - If the configurations of the local device are proper, go to Step 3.
 2. Delete the configurations that cause the interruption of the peer relationship.
 3. Check whether the BGP connection is reset. If the BGP connection is reset, wait for a while and then check whether the BGP connection is re-established.
 - If the BGP connection is not reset, go to Step 4.
 - If the BGP connection is reset, wait for a while and then check whether the BGP connection is re-established. If the BGP connection is not re-established, go to Step 4. Collect alarm information and configuration information, and then contact technical support personnel.
- Cause 2: BGP receive notification
 1. Run the `display bgp peer ip-address log-info` command to check the notification information when the BGP connection is torn down.
 - If the value of Error Code in the Notification packet is 4, the BGP Holdtimer expires and no Keepalive packet is received. In this case, go to Step 3.
 - If the value of Error Code in the Notification packet is 5, an error occurs on the BGP FSM. Go to step 17.
 - If the value of Error Code in the Notification packet is 6, BGP proactively terminated the connection. In this case, go to Step 2.
 2. Run the `display bgp peer ip-address log-info` command to check whether the notification is sent by the device that generates the alarm.
 - Yes: Go to Step 3.
 - If no, go to Step 4.
 3. Run the `ping` command to check whether the IP address of the BGP peer can be pinged.

- Yes: Go to Step 4.
 - If no, go to Step 5.
4. Run the `display cpu-usage` command to check whether the CPU usage is too high.
- Yes: Go to Step 17.
 - If no, go to Step 6.
5. Run the `display ip routing-table` command to check whether the BGP peer address routing table exists.
- Yes: Go to Step 7.
 - If no, go to Step 8.
6. Run the `display acl` command to check whether an ACL is configured to disable TCP port 179.
- If yes, delete the ACL that denies TCP port 179.
 - If no, go to Step 9.
7. Run the `display interface` command to check whether the outbound interface of the route is Up.
- Yes: Go to Step 17.
 - If not, go to step 10.
8. Check the configuration information for the origin of the route to the BGP peer address.
- If the route source is OSPF, go to Step 11.
 - If the route originates from IS-IS, go to Step 12.
9. Check the BGP configuration to see whether the loopback interface is applied.
- Yes: Go to Step 13.
 - If not, go to step 14.
10. Check whether the shutdown command is run on the interface.
- If so, run the `undo shutdown` command on the interface. If the alarm persists, go to Step 13.
 - If not, go to Step 17.
11. Run the `display ospf peer` command to check whether the OSPF peer relationship is established.
- Yes: Go to Step 17.
 - If not, see the procedure for handling the OSPF_1.3.6.1.2.1.14.16.2.2 ospfNbrStateChange alarm.
12. Run the `display isis peer` command to check whether the IS-IS peer relationship is established.
- Yes: Go to Step 17.
 - If not, see the procedure for handling the ISIS_1.3.6.1.3.37.2.0.17 isisAdjacencyChange alarm.
13. Check whether a source address is specified for the BGP connection.
- Yes: Go to Step 14.
 - If not, run the `peer connect-interface` command to specify the source address used to initiate a BGP connection.

14. If the BGP peer is an EBGP peer and multiple hops exist between EBGP peers, check whether the peer ebgp-max-hop command is configured.

- Yes: Go to Step 15.
- If not, run the peer ebgp-max-hop command.

15. If the peer valid-ttl-hops *hops* command is configured, check whether the TTL of the packet received from the peer is within the range of 255-hops+1 to 255.

- Yes: Go to Step 16.
- If not, reconfigure the peer valid-ttl-hops *hops* command to ensure that the TTL of the packets sent to the peer is within the range of 255-hops+1 to 255.

16. Contact the maintenance personnel of the peer device to check whether BGP is reset on the peer device, whether the peer enable command is run in another address family view on the local device, or whether BGP connection parameters are set. If any of these operations has been performed, wait for a while and then check whether the alarm is cleared. If the alarm persists, go to Step 17.

17. Collect alarm and configuration information, and contact technical support personnel.

- Cause 3: BGP receive error packet

1. Run the display bgp peer *ip-address* log-info command to check the Notification packet sent by the local device when the BGP peer relationship is interrupted.

- If the value of the Error Code field in the Notification packet is 1, a packet with an error header has been received. Go to Step 2.
- If the value of the Error Code field in the Notification packet is 2, an error Open packet has been received. Go to Step 2.
- If the value of the Error Code field in the Notification packet is 3, an error Update packet has been received. Go to Step 2.

2. Collect alarm information and configuration information, and then contact technical support personnel.

- Cause 4: BGP hold timer expire

1. Run the ping command to check whether the IP address of the BGP peer can be pinged.

- If so, go to step 2.
- If no, go to Step 3.

2. Run the display cpu-usage command to check whether the CPU usage is too high.

- Yes: Go to Step 15.
- If no, go to Step 4.

3. Run the display ip routing-table command to check whether the BGP peer address routing table exists.

- Yes: Go to Step 5.
- If no, go to Step 6.

4. Run the display acl command to check whether an ACL is configured to disable TCP port 179.

- If yes, delete the ACL that denies TCP port 179.
 - If no, go to Step 7.
5. Run the display interface command to check whether the outbound interface of the route is Up.
- Yes: Go to Step 15.
 - If no, go to Step 8.
6. Check the source of the route to the BGP peer address.
- If the route source is OSPF, go to Step 9.
 - If the route originates from IS-IS, go to Step 10.
7. Check the BGP configuration to see whether the loopback interface is applied.
- Yes: Go to Step 11.
 - If no, go to Step 12.
8. Check whether the shutdown command is run on the interface.
- Run the undo shutdown command on the interface. If the alarm persists, go to Step 11.
 - If no, go to Step 15.
9. Run the display ospf peer command to check whether the OSPF peer relationship is established.
- Yes: Go to Step 15.
 - If not, see the procedure for handling the OSPF_1.3.6.1.2.1.14.16.2.2 ospfNbrStateChange alarm.
10. Run the display isis peer command to check whether the IS-IS peer relationship is established.
- Yes: Go to Step 15.
 - If not, see the procedure for handling the ISIS_1.3.6.1.3.37.2.0.17 isisAdjacencyChange alarm.
11. Check whether a source address is specified for the BGP connection.
- Yes: Go to Step 12.
 - If not, run the peer connect-interface command to specify the source address used to initiate a BGP connection.
12. If the BGP peer is an EBGP peer and multiple hops exist between EBGP peers, check whether the peer ebgp-max-hop command is configured.
- Yes: Go to Step 13.
 - If not, run the peer ebgp-max-hop command.
13. If the peer valid-ttl-hops *hops* command is configured, check whether the TTL of the packet received from the peer is within the range of 255-hops+1 to 255.
- Yes: Go to Step 14.
 - If not, reconfigure the peer valid-ttl-hops *hops* command to ensure that the TTL of the packets sent to the peer is within the range of 255-hops+1 to 255.
14. Contact the maintenance personnel of the peer device to check whether BGP is reset on the peer device, whether the peer enable command is run in

another address family view on the local device, or whether BGP connection parameters are set. If any of these operations has been performed, wait for a while and then check whether the alarm is cleared. If the alarm persists, go to Step 15.

15. Collect alarm and configuration information, and contact technical support personnel.

- Cause 5: BGP remote peer not reachable
 1. Run the ping command to check whether the IP address of the BGP peer can be pinged.
 - If so, go to step 2.
 - If no, go to Step 3.
 2. Run the display cpu-usage command to check whether the CPU usage is too high.
 - Yes: Go to Step 15.
 - If no, go to Step 4.
 3. Run the display ip routing-table command to check whether the BGP peer address routing table exists.
 - Yes: Go to Step 5.
 - If no, go to Step 6.
 4. Run the display acl command to check whether an ACL is configured to disable TCP port 179.
 - If yes, delete the ACL that denies TCP port 179.
 - If no, go to Step 7.
 5. Run the display interface command to check whether the outbound interface of the route is Up.
 - Yes: Go to Step 15.
 - If no, go to Step 8.
 6. Check the source of the route to the BGP peer address.
 - If the route source is OSPF, go to Step 9.
 - If the route originates from IS-IS, go to Step 10.
 7. Check the BGP configuration to see whether the loopback interface is applied.
 - Yes: Go to Step 11.
 - If no, go to Step 12.
 8. Check whether the shutdown command is run on the interface.
 - Run the undo shutdown command on the interface. If the alarm persists, go to Step 11.
 - If no, go to Step 15.
 9. Run the display ospf peer command to check whether the OSPF peer relationship is established.
 - Yes: Go to Step 15.
 - If not, see the procedure for handling the OSPF_1.3.6.1.2.1.14.16.2.2 ospfNbrStateChange alarm.

10. Run the `display isis peer` command to check whether the IS-IS peer relationship is established.
 - Yes: Go to Step 15.
 - If not, see the procedure for handling the `ISIS_1.3.6.1.3.37.2.0.17 isisAdjacencyChange` alarm.
 11. Check whether a source address is specified for the BGP connection.
 - Yes: Go to Step 12.
 - If not, run the `peer connect-interface` command to specify the source address used to initiate a BGP connection.
 12. If the BGP peer is an EBGP peer and multiple hops exist between EBGP peers, check whether the `peer ebgp-max-hop` command is configured.
 - Yes: Go to Step 13.
 - If not, run the `peer ebgp-max-hop` command.
 13. If the `peer valid-ttl-hops hops` command is configured, check whether the TTL of the packet received from the peer is within the range of $255-hops+1$ to 255.
 - Yes: Go to Step 14.
 - If not, reconfigure the `peer valid-ttl-hops hops` command to ensure that the TTL of the packets sent to the peer is within the range of $255-hops+1$ to 255.
 14. Contact the maintenance personnel of the peer device to check whether BGP is reset on the peer device, whether the `peer enable` command is run in another address family view on the local device, or whether BGP connection parameters are set. If any of these operations has been performed, wait for a while and then check whether the alarm is cleared. If the alarm persists, go to Step 15.
 15. Collect alarm and configuration information, and contact technical support personnel.
- Cause 6: BGP direct connect-interface down
 1. Check whether the shutdown command is run on the directly connected interface.
 2. Collect alarm information and configuration information, and then contact technical support personnel.
 - Cause 7: BGP route exceed the maximum number allowed
 1. Check whether the `peer route-limit` command is run and whether the number of routes exceeds the upper threshold.
 - If the command is run and the number of received routes exceeds the upper threshold, go to Step 2.
 - If the command is not run or the command is run but the number of received routes does not exceed the upper threshold, go to Step 3.
 2. Check whether the `peer route-limit` command is necessary. If the command is necessary, reduce routes to ensure that the number of routes is smaller than the upper threshold.
 3. Collect alarm information and configuration information, and then contact technical support personnel.

Clearing

After the fault is rectified, the system clears this alarm, removing the need to manually clear it. This alarm will not be displayed on the **Current Alarms** page.

3.5.2.2 ALM-15794956 hwBgpPeerAddrFamilyRouteThresholdExceed

Description

The number of routes received from peers in a BGP address family reached the alarm threshold. (AddressFamily=[AddressFamily], MaxRouteNumber=[RouteLimitNum], AlarmThreshold=[RouteLimitThreshold], BGP instance name=[InstanceName])

The number of routes received from peers in a BGP address family reached the alarm threshold.

Attribute

Alarm ID	OID	Alarm Severity	Alarm Type
15794956	1.3.6.1.4.1.2011.5.25.177.1.3.29	Major	Communication alarm

Parameters

Name	Meaning
AddressFamily	Address family
RouteLimitNum	The maximum route number
RouteLimitThreshold	Alarm threshold
InstanceName	BGP instance name. "-" indicates the default BGP instance, and other values indicate multiple instances.

Impact on the System

The number of routes received from peers in the address family has reached the alarm threshold.

Possible Causes

The number of routes received from peers in a BGP address family reached the alarm threshold.

Procedure

1. Reduce the number of routes sent by the peer end. Then, check whether the alarm is cleared. That is, check whether the matching clear alarm (hwBgpPeerAddrFamilyRouteThresholdExceedClear) is generated.
- If the clear alarm is generated, go to Step 3.

• If the clear alarm is not generated, go to Step 2.
2. Collect alarm information and configuration information, and then contact technical support personnel.
3. End.

Clearing

After the fault is rectified, the system clears this alarm, removing the need to manually clear it. This alarm will not be displayed on the **Current Alarms** page.

3.5.2.3 ALM-15795089 hwBgpPeerAddrFamilyRouteExceed

Description

The number of routes received from peers in a BGP address family reached the maximum value. (Address Family=[AddressFamily], MaxRouteNumber=[RouteLimitNum], BGP instance name=[InstanceName])

The number of routes received from peers in a BGP address family reached the maximum value.

Attribute

Alarm ID	OID	Alarm Severity	Alarm Type
15795089	1.3.6.1.4.1.2011.5.25.177.1.3.31	Major	Communication alarm

Parameters

Name	Meaning
AddressFamily	Address family
RouteLimitNum	The maximum route number
InstanceName	BGP instance name. "-" indicates the default BGP instance, and other values indicate multiple instances.

Impact on the System

The number of routes received from peers in the address family has reached the specification, and no more new routes can be received.

Possible Causes

The number of routes received from peers in a BGP address family reached the maximum value.

Procedure

1. Reduce the number of routes sent by the peer end. Then, check whether the alarm is cleared. That is, check whether the matching clear alarm (hwBgpPeerAddrFamilyRouteExceedClear) is generated.

- If the clear alarm is generated, go to Step 3.
- If the clear alarm is not generated, go to Step 2.

2. Collect alarm information and configuration information, and then contact technical support personnel.

3. End.

Clearing

After the fault is rectified, the system clears this alarm, removing the need to manually clear it. This alarm will not be displayed on the **Current Alarms** page.

3.5.2.4 ALM-15795185 hwConnectionDownReport

Description

The connection has entered the down state. (ConnectionID=[ConnectionID], DestSiteID=[DestSiteID], SrcSiteID=[SrcSiteID], DestTNPID=[DestTNPID], SrcTNPID=[SrcTNPID],DownReason=[DownReason])

The EVPN connection went Down.

Attribute

Alarm ID	OID	Alarm Severity	Alarm Type
15795185	1.3.6.1.4.1.2011.5.25.241.6.3.2	Major	Quality of service alarm

Parameters

Name	Meaning
ConnectionID	Connection ID.

Name	Meaning
DestSiteID	Name of the destination site.
SrcSiteID	Name of the source site.
DestTNPID	Destination TNP.
SrcTNPID	Source TNP.
DownReasonID	Cause ID.

Impact on the System

Service may be interrupted.

Possible Causes

- Cause 1:The site tunnel route is deleted.
- Cause 2:The DH group does not match.
- Cause 3:The DH group is changed.
- Cause 4:The TNP is deleted.
- Cause 5:The TNP status changes to down.
- Cause 6:The TNP weight is changed.
- Cause 7:KA detection fails.
- Cause 8:Reset by user.

Procedure

1. Check whether the service route to the corresponding site is deleted.
 - a. Run the display tunnel all command to view information about all tunnels.
 - b. Run the display tunnel tunnel-id command to view information about a specified SD-WAN tunnel and check whether the corresponding service route exists.
 - If the route does not exist, configure a route to the corresponding site.
 - If the route exists, collect alarm and configuration information, and contact technical support personnel.
2. Check whether the DH group of the local device matches that of the peer device.

Run the **display ipsec p2mp-policy** command to check the DH groups used by the key exchange algorithm in the IPSec P2MP security policies of the local and peer devices. If the DH groups of the two devices are different and one device uses the strict mode, the DH groups cannot match. Configure the same DH group or disable the strict mode.

3. Run the display **ipsec p2mp-policy** command to check the DH group used by the key exchange algorithm in the IPsec P2MP security policy of the peer device. Check whether the DH group is changed.
4. Run the display **evpn site-tnp site-id** command to check whether the TNP of the peer device is deleted.
 - If so, configure TNP information.
 - If not, collect alarm and configuration information, and contact technical support personnel
5. Check whether the TNP of the local device is bound to an interface.
 - a. Run the **display evpn site-tnp site-id verbose** command to check whether the TNP of the local device is bound to an interface.
 - If so, go to step 3.
 - If not, go to step 2.
 - b. Configure the source interface of the TNP.
 - c. Check whether the protocol status of the physical interface bound to the TNP is Up.
 - d. Check whether the shutdown command is run on the interface.
6. Run the **display evpn site-tnp site-id verbose** command to check whether the TNP's weight is changed.
7. Check the interfaces bound to the TNP.
 - a. Check whether the interfaces bound to the TNP can ping each other.
 - If so, go to step 3.
 - If not, go to step 2.
 - b. Check whether the intermediate transport network is faulty.
 - c. Collect alarm and configuration information, and contact technical support personnel.
8. Check whether BGP or EVPN connections are reset on the local device.

Clearing

After the fault is rectified, the system clears this alarm, removing the need to manually clear it. This alarm will not be displayed on the **Current Alarms** page.

3.5.2.5 ALM-15795206 hwConnectionThresholdExceed

Description

The number of connections has exceeded the threshold. (MaximumNumber = [MaximumNumber], CurrentConnecionNumber = [CurrentConnecionNumber], ThresholdPercent = [ThresholdPercent], ResumeThresholdPercent = [ResumeThresholdPercent])

The number of SD-WAN EVPN connections reaches 80% of the maximum number.

Attribute

Alarm ID	OID	Alarm Severity	Alarm Type
15795206	1.3.6.1.4.1.2011.5.25.241.6.3.5	Minor	Quality of service alarm

Parameters

Name	Meaning
MaximumNumber	Maximum number of connections supported by the device.
CurrentConnecionNumber	Number of current connections of a device.
ThresholdPercent	Specifies the upper threshold percentage. The value is fixed at 80%.
ResumeThresholdPercent	Indicates the percentage of the link recovery threshold. The value is fixed at 50%.

Impact on the System

New connections may be not established.

Possible Causes

- The size of sites is too large. The device needs to establish connections with all sites, which beyonds the threshold number of the device can support.

Procedure

1. Adjust the topology between sites on the iMaster NCE-Campus page, connect the site to the Hub site, and relay packages through the Hub site. Check recover alarm can be generated.
 - If so, go to step 3.
 - If not, go to step 2.
2. Collect alarm information and configuration information, and then contact technical support personnel.
3. End.

Clearing

After the fault is rectified, the system clears this alarm, removing the need to manually clear it. This alarm will not be displayed on the **Current Alarms** page.

3.5.2.6 ALM-15795205 hwConnectionMaxExceed

Description

The number of connections has reached 100% of the maximum number.
(MaximumNumber = [MaximumNumber])

SD-WAN EVPN connection reaches 100% of the maximum number.

Attribute

Alarm ID	OID	Alarm Severity	Alarm Type
15795205	1.3.6.1.4.1.2011.5 .25.241.6.3.3	Major	Quality of service alarm

Parameters

Name	Meaning
MaximumNumber	The maximum number of connections to device support.

Impact on the System

Some connections of sites may be not work.

Possible Causes

- The size of sites is too large. The device needs to establish connections with all sites, which beyond the number of the device can support.

Procedure

1. Adjust the topology between sites on the iMaster NCE-Campus page, connect the site to the Hub site, and relay packages through the Hub site. Check recover alarm can be generated.
 - If so, go to step 3.
 - If not, go to step 2.
2. Collect alarm information and configuration information, and then contact technical support personnel.
3. End.

Clearing

After the fault is rectified, the system clears this alarm, removing the need to manually clear it. This alarm will not be displayed on the **Current Alarms** page.

3.5.2.7 ALM-15795258 hwSPRInstanceReport

Description

The path of SPR instance changed. (DestSiteIndex = [DestSiteIndex], VpnInstance = [VpnInstance], PolicyName = [PolicyName], PreviousLink = [PreviousLink], PreviousLinkLoss = [PreviousLinkLoss], PreviousLinkDelay = [PreviousLinkDelay], PreviousLinkJitter = [PreviousLinkJitter], PreviousLinkCMI = [PreviousLinkCMI], CurrentLink = [CurrentLink], ChangedReason = [ChangedReason])

The path of the SPR instance changed.

Attribute

Alarm ID	OID	Alarm Severity	Alarm Type
15795258	1.3.6.1.4.1.2011.5.25.241.2.4.2	Minor	Quality of service alarm

Parameters

Name	Meaning
DestSiteIndex	Name of the destination site.
VpnInstance	VPN instance name.
PolicyName	SPR policy name.
PreviousLink	Name of the link selected by the SPR instance before the link switchover.
PreviousLinkLoss	Packet loss rate of the link selected by the SPR instance before the link switchover.
PreviousLinkDelay	Delay of the link selected by the SPR instance before the link switchover.
PreviousLinkJitter	Jitter of the link selected by the SPR instance before the link switchover.
PreviousLinkCMI	Comprehensive metric value of the link selected by the SPR instance before the link switchover.

Name	Meaning
CurrentLink	Name of the link selected by the SPR instance after the link switchover.
ChangedReason	Cause of the link switchover

Impact on the System

- This is a normal phenomenon and has no impact on the system.
- This is a normal phenomenon and has no impact on the system.
- This is a normal phenomenon and has no impact on the system.
- This is a normal phenomenon and has no impact on the system.
- This is a normal process and has no impact on the system.
- This is a normal process and has no impact on the system.
- This is a normal process and has no impact on the system.
- This is a normal process and has no impact on the system.

Possible Causes

- Cause 1: The link delay exceeded the threshold configured in the policy.
- Cause 2: The link loss exceeded the threshold configured in the policy.
- Cause 3: The link jitter exceeded the threshold configured in the policy.
- Cause 4: The link cmi exceeded the threshold configured in the policy.
- Cause 5: The link status changed.
- Cause 6: The selected link was unavailable.
- Cause 7: Traffic was switched back from a low-priority link to a high-priority link.
- Cause 8: SPR chose the best link from poor quality.

Procedure

- Cause 1: The link delay exceeded the threshold configured in the policy.
 - a. Run the **display spr-policy** command to check whether the delay threshold in the SPR policy is correct.
 - If the configuration is incorrect, run the **set delay threshold** command to set a proper delay threshold, and then go to Step 4.
 - If the configuration is correct, go to Step 2.
 - b. Check the status of the transport network.
 - If the network has a long delay, the link switchover is normal. Go to step 4.
 - If the fault is not caused by the network, go to Step 3.
 - c. Collect alarm, log, and configuration information, and contact technical support personnel.

- d. End.
- Cause 2: The link loss exceeded the threshold configured in the policy.
 - a. Run the **display spr-policy** command to check whether the packet loss rate threshold in the SPR policy is correct.
 - If the configuration is incorrect, run the **set loss threshold** command to set a proper threshold for the policy, and then go to Step 4.
 - If the configuration is correct, go to Step 2.
 - b. Check the status of the transport network.
 - If packet loss occurs on the network, the link switchover is normal. Go to step 4.
 - If the fault is not caused by the network, go to Step 3.
 - c. Collect alarm, log, and configuration information, and contact technical support personnel.
 - d. End.
- Cause 3: The link jitter exceeded the threshold configured in the policy.
 - a. Run the **display spr-policy** command to check whether the jitter threshold of the SPR policy is correct.
 - If not, run the **set jitter threshold** command to set a proper jitter threshold, and then go to step 4.
 - If the configuration is correct, go to Step 2.
 - b. Check the status of the transport network.
 - If packet loss occurs on the network, the link switchover is normal. Go to step 4.
 - If the fault is not caused by the network, go to Step 3.
 - c. Collect alarm, log, and configuration information, and contact technical support personnel.
 - d. End.
- Cause 4: The link cmi exceeded the threshold configured in the policy.
 - a. Run the **display spr-policy** command to check whether the jitter threshold of the SPR policy is correct.
 - If not, run the **set jitter threshold** command to set a proper jitter threshold, and then go to step 4.
 - If the configuration is correct, go to Step 2.
 - b. Check the status of the transport network.
 - If the network quality is poor when the switchover occurs, the link switchover is normal. In this case, go to step 4.
 - If the fault is not caused by the network, go to Step 3.
 - c. Collect alarm, log, and configuration information, and contact technical support personnel.

d. End.

- This alarm message is informational only, and no action is required.
- This alarm message is informational only, and no action is required.
- This alarm message is informational only, and no action is required.
- This alarm message is informational only, and no action is required.

Clearing

The alarm needs to be cleared manually.

3.5.2.8 ALM-15795318 hwSessExceed

Description

The number of session resources exceeds the limit. (Current usage=[Usage]%, Threshold=[Threshold]%)

When the number of current sessions reaches the upper limit, the device generates an alarm.

Attribute

Alarm ID	OID	Alarm Severity	Alarm Type
15795318	1.3.6.1.4.1.2011.5.25.227.2.1.69	Major	Quality of service alarm

Parameters

Name	Meaning
Usage	Ratio of the number of current sessions to the maximum number of sessions
Threshold	Alarm threshold of session resources

Impact on the System

Services are affected.

Possible Causes

The number of forwarding session tables in the current device is 100% of the number of specifications.

Procedure

Check whether the service configuration exceeds the specifications and contact technical support personnel.

Clearing

After the fault is rectified, the system clears this alarm, removing the need to manually clear it. This alarm will not be displayed on the **Current Alarms** page.

3.5.2.9 ALM-15795117 hwSystemRollback

Description

System rollback. (FileName=[SoftwareName], Version=[Version], Reason=[FailReason])

The system fails to start , and the software rolls back to the old version.

Attribute

Alarm ID	OID	Alarm Severity	Alarm Type
15795117	1.3.6.1.4.1.2011.5.2 5.219.2.11.3	Warning	Processing error alarm

Parameters

Name	Meaning
SoftwareName	The software package name before the rollback
Version	The version before the rollback
FailReason	Error reason

Impact on the System

- Cause 1:The system software supports only the service features of the current version after the startup succeeds.
- Cause 2: After the system software is started from the backup area, the user cannot add or delete files on the backup area, and cannot set the next startup package as a file on the backup area

Possible Causes

- Cause 1: Rollback occurs on the system.

- Cause 2: The system starts from the backup area.

Procedure

- Cause 1: Rollback occurs on the system.
 - a. Run the `dir` command to check the file system.
 - If the storage medium is unavailable, the storage medium is damaged. Go to [2](#).
 - If the storage medium is available, system software is faulty and cannot start the system. Go to [3](#).
 - b. Check the storage medium saved in the system software.
 - If the storage medium is an SD card or a USB disk, replace it and restart the upgrade. If the upgrade fails, go to [3](#).
 - If the storage medium is flash, record the device type and number, collect alarm information and configuration information, and then contact technical support personnel.
 - c. Collect operation results, alarm information, and configuration information, and then contact technical support personnel.
- Cause 2: The system starts from the backup area.
 - a. Run the **display startup** command in the user view to view information about the system software and configuration files started by the current device. The display shows that the storage path of the system software or configuration file used for this startup is the backup area, indicating that the system starts from the backup area.
 - b. After starting from the standby area, the user cannot select the files in the standby area to set the next startup. Please format the root directory of the main area. After the main area is repaired, copy the system software to the main area directory and perform the upgrade. If the upgrade still fails, go to [3](#).
 - c. Collect operation results, alarm information, and configuration information, and then contact technical support personnel.

Clearing

The alarm needs to be cleared manually.

3.5.2.10 ALM-15794965 hwSrPolicyDown

Description

The SR Policy went down. (hwSrPolicyEndpoint=[SrPolicyEndpoint], hwSrPolicyColor=[SrPolicyColor], hwSrPolicyDownReason=[DownReason])

The SR Policy went down.

Attribute

Alarm ID	OID	Alarm Severity	Alarm Type
15794965	1.3.6.1.4.1.2011.5.2 5.359.2.4	Major	Communication alarm

Parameters

Name	Meaning
SrPolicyEndpoint	Endpoint
SrPolicyColor	Color value
DownReason	Down Reason

Impact on the System

Traffic will be switched to another tunnel or fail to be forwarded.

Possible Causes

- Cause 1: The SR Policy was manually shut down.
- Cause 2: No candidate path was available.

Procedure

- Cause 1:
Run the **undo shutdown** command in the **SR Policy** view.
- Cause 2:
 - a. Check links.
 - b. Configure a candidate path with valid segment lists for the SR Policy.

Clearing

After the fault is rectified, the system clears this alarm, removing the need to manually clear it. This alarm will not be displayed on the **CurrentAlarms** page.

3.5.2.11 ALM-15794966 hwSrPolicyResourceThresholdExceed

Description

The number of used SR Policy resources exceeded the upper threshold.
(hwSrPolicyResourceType=[SrPolicyResourceType],
hwResourceCurrentCount=[ResourceCurrentCount],
hwResourceThresholdUpperLimit=[ResourceThresholdUpperLimit],

hwResourceThresholdLowerLimit=[ResourceThresholdLowerLimit],
hwResourceTotalCount=[ResourceTotalCount])

The number of used SR Policy resources exceeded the upper threshold.

Attribute

Alarm ID	OID	Alarm Severity	Alarm Type
15794966	1.3.6.1.4.1.2011.5.2 5.359.2.6	Warning	Communication alarm

Parameters

Name	Meaning
SrPolicyResourceType	SR Policy resource type • srv6TePolicy(0) • srv6TePolicySegmentList(1) • srMplsTePolicy(3) • srMplsTePolicySegmentList(4) • srv6TePolicyGroup(5)
ResourceCurrentCount	Number of currently used SR Policy resources
ResourceThresholdUpperLimit	Upper threshold for the number of used SR Policy resources
ResourceThresholdLowerLimit	Lower threshold for the number of used SR Policy resources
ResourceTotalCount	Maximum number of SR Policy resources that can be used

Impact on the System

If more SR Policy resources of the specified type are used, services may be adversely affected.

Possible Causes

The number of used SR Policy resources of the specified type reached the upper threshold.

Procedure

Check the threshold-crossing information of specific SR Policy resources based on SrPolicyResourceType.

Clearing

After the fault is rectified, the system clears this alarm, removing the need to manually clear it. This alarm will not be displayed on the **CurrentAlarms** page.

3.5.2.12 ALM-15794967 hwSrPolicyResourceTotalCountExceed

Description

The total number of SR Policy resources exceeded the maximum number of SR Policy resources that can be used.

(hwSrPolicyResourceType=[SrPolicyResourceType],
hwResourceCurrentCount=[ResourceCurrentCount],
hwResourceTotalCount=[ResourceTotalCount])

The total number of SR Policy resources exceeded the maximum number of SR Policy resources that can be used.

Attribute

Alarm ID	OID	Alarm Severity	Alarm Type
15794967	1.3.6.1.4.1.2011.5.2 5.359.2.8	Major	Communication alarm

Parameters

Name	Meaning
SrPolicyResourceType	SR Policy resource type • srv6TePolicy(0) • srv6TePolicySegmentList(1) • srMplsTePolicy(3) • srMplsTePolicySegmentList(4) • srv6TePolicyGroup(5)
ResourceCurrentCount	Number of currently used SR Policy resources
ResourceTotalCount	Maximum number of SR Policy resources that can be used
EntityOperStatus	Alarm status information
ReasonDsp	Alarm cause

Impact on the System

If more SR Policy resources of the specified type are used, services may be adversely affected.

Possible Causes

The total number of SR Policy resources of the specified type exceeded the maximum number of SR Policy resources that can be used.

Procedure

Check the threshold-crossing information of specific SR Policy resources based on SrPolicyResourceType.

Clearing

After the fault is rectified, the system clears this alarm, removing the need to manually clear it. This alarm will not be displayed on the **CurrentAlarms** page.

3.5.2.13 ALM-15795368 hwSiteDisconnect

Description

All connections between sites have entered down state.
(SrcSite=[SrcSite],DestSite=[DestSite],CurrentConnectionNumber=[CurrentConnectionNumber])

All links between sites are unavailable.

Attribute

Alarm ID	OID	Alarm Severity	Alarm Type
15795368	1.3.6.1.4.1.2011.5.25.241.6.3.7	Major	Quality of service alarm

Parameters

Name	Meaning
SrcSite	Name of the source site.
DestSite	Name of the destination site.
CurrentConnectionNumber	Number of current connections of a site.

Impact on the System

- Cause 1: The site tunnel route is deleted.
Services are interrupted.
- Cause 2: The DH group does not match.
Service may be interrupted.
- Cause 3: The DH group is changed.
Services may flap.
- Cause 4: The TNP is deleted.
Service may be interrupted.
- Cause 5: The TNP status changes to down.
Service may be interrupted.
- Cause 6: The TNP weight is changed.
Services may flap.
- Cause 7: KA detection fails.
Service may be interrupted.
- Cause 8: Reset by user.
Services may flap.

Possible Causes

- Cause 1: The site tunnel route is deleted.
- Cause 2: The DH group does not match.
- Cause 3: The DH group is changed.
- Cause 4: The TNP is deleted.
- Cause 5: The TNP status changes to down.
- Cause 6: The TNP weight is changed.
- Cause 7: KA detection fails.
- Cause 8: Reset by user.

Procedure

- Cause 1: The site tunnel route is deleted.
Check whether the service route to the corresponding site is deleted.
 - a. Run the **display tunnel all** command to check information about all tunnels.
 - b. Run the **display tunnel tunnel-id** command to check SD-WAN tunnel information one by one and check whether corresponding service routes exist.
 - If no, configure the corresponding site route.
 - If yes, collect alarm and configuration information and contact technical support personnel.
- Cause 2: The DH group does not match.

Check whether the DH group configured on the local device matches that configured on the peer device.

Run the **display ipsec p2mp-policy** command to check the Key-Exchange information on both ends of the IPsec tunnel.

If the DH groups of the two communication parties are different and one party uses the strict mode, the DH groups of the two communication parties do not match.

Configure the same DH group or disable the strict mode.

- Cause 3: The DH group is changed.

Run the **display ipsec p2mp-policy** command to check the DH group used by the key exchange algorithm in the IPsec P2MP security policy of the peer device. Check whether the DH group is changed.

- Cause 4: The TNP is deleted.

- a. Run the **display evpn site-tnp site-id** command to check whether the TNP of the peer device is deleted.

- If yes, configure TNP information.
- If no, collect alarm and configuration information and contact technical support personnel.

- Cause 5: The TNP status changes to down.

- a. Run the **display evpn site-tnp site-id verbose** command to check whether the TNP on the local device is bound to an interface.

- Yes: Go to Step 3.
- If not, go to step 2.

- b. Configure the source interface of the TNP.
- c. Check whether the protocol status of the physical interface bound to the TNP is Up.
- d. Check whether the **shutdown** command is run on the interface.

- Cause 6: The TNP weight is changed.

- a. Run the **display evpn site-tnp site-id verbose** command to check whether the TNP's weight is changed.

- Cause 7: KA detection fails.

- a. Check whether the interfaces bound to the TNP can ping each other.

- If so, go to step 3.
- If not, go to step 2.

- b. Check whether the intermediate transport network is faulty.
- c. Collect alarm and configuration information, and contact technical support personnel.

- Cause 8: Reset by user.

Check whether BGP or EVPN connections are reset on the local device.

Clearing

After the fault is rectified, the system clears this alarm, removing the need to manually clear it. This alarm will not be displayed on the **CurrentAlarms** page.

3.5.2.14 ALM-15795445 hwConnectionPolicyApplyFail

Description

he connection policy failed to apply.
(ConnectionID=[ConnectionID],DestSiteID=[DestSiteID],SrcSiteID=[SrcSiteID],DestTNPID=[DestTNPID],SrcTNPID=[SrcTNPID],FailReason=[FailReason])

The policy failed to apply to an SD-WAN EVPN connection.

Attribute

AlarmID	Alarm OID	Alarm Severity	Alarm Type
15795445	1.3.6.1.4.1.2011.5.25.241.6.3.9	Major	Quality of service alarm

Parameters

Name	Meaning
ConnectionID	Connection ID.
DestSiteID	ID of the destination site.
SrcSiteID	ID of the source site.
DestTNPID	ID of the destination TNP.
SrcTNPID	ID of the source TNP.
FailReason	Failure cause.

Impact on the System

Some services are unavailable.

Possible Causes

ACL resources or QoS queues on the device are insufficient.

Procedure

Delete other services that occupy ACLs and QoS queues to release some resources.

Related Information

None.

3.5.2.15 ALM-215031809 hwSystemRollback

Description

System rollback. (FileName=[SoftwareName], Version=[Version], Reason=[FailReason])

The system fails to start , and the software rolls back to the old version.

Attribute

AlarmID	Alarm OID	Alarm Severity	Alarm Type
215031809	1.3.6.1.4.1.2011.5.25.241.6.3.9	Major	Quality of service alarm

Parameters

Name	Meaning
SoftwareName	The software package name before the rollback
Version	The version before the rollback
FailReason	Error reason

Impact on the System

- Cause 1: Rollback occurs on the system.
The system software supports only the service features of the current version after the startup succeeds.
- Cause 2: The system starts from the backup area.
After the system software is started from the backup area, the user cannot add or delete files on the backup area, and cannot set the next startup package as a file on the backup area.

Possible Causes

- Cause 1: Rollback occurs on the system.
- Cause 2: The system starts from the backup area.

Procedure

- Cause 1: Rollback occurs on the system.

- a. Run the dir command to check the file system.
 - If the storage medium is unavailable, the storage medium is damaged. Go to step 2.
 - If the storage medium is available, system software is faulty and cannot start the system. Go to step 3.
- b. Check the storage medium saved in the system software.
 - If the storage medium is an SD card or a USB disk, replace it and restart the upgrade. If the upgrade fails, go to step 3.
 - If the storage medium is flash, record the device type and number, collect alarm information and configuration information, and then contact technical support personnel.
- c. Collect operation results, alarm information, and configuration information, and then contact technical support personnel.
- Cause 2: The system starts from the backup area.
 - a. Run the display startup command in the user view to view information about the system software and configuration files started by the current device. The display shows that the storage path of the system software or configuration file used for this startup is the backup area, indicating that the system starts from the backup area. .
 - b. After starting from the standby area, the user cannot select the files in the standby area to set the next startup. Please format the root directory of the main area. After the main area is repaired, copy the system software to the main area directory and perform the upgrade. If the upgrade still fails, go to step 3
 - c. Collect operation results, alarm information, and configuration information, and then contact technical support personnel.

Related Information

None.

3.5.2.16 ALM-15795156 HostUnitLinkAbnormal

Description

Host unit link abnormal. (LocalHostUnitName=[LocalHostUnitName], RemoteHostUnitName=[RemoteHostUnitName], PlaneType=[PlaneType], Reason=[Reason])

Host Unit Link Abnormal.

Attribute

AlarmID	Alarm OID	Alarm Severity	Alarm Type
15795156	1.3.6.1.4.1.2011.5.25.241.6.3.9	Major	Communication alarm

Parameters

Name	Meaning
LocalHostUnitName	Indicates the name of the host unit that reports the alarm.
RemoteHostUnitName	Peer Host Unit Name.
PlaneType	Plane Type.
Reason	Reason.

Impact on the System

Basic communication functions and services of the system are affected.

Possible Causes

The link becomes down or subhealthy.

Procedure

1. Check the network cable. If the network cable is faulty, replace it and check whether the alarm is cleared.
 - Yes: The alarm handling is complete, and no further action is required.
 - No: Go to 2.
2. Decrease service traffic gradually, and wait about 3 minutes. Then check whether the alarm is cleared.
 - Yes: The alarm handling is complete, and no further action is required.
 - No: Go to 3.
3. Collect alarm information and configuration information, and then contact technical support personnel.

Related Information

None.

3.5.2.17 ALM-15795527 VMResourceInconsist

Description

Host unit link abnormal. (LocalHostUnitName=[LocalHostUnitName], RemoteHostUnitName=[RemoteHostUnitName], PlaneType=[PlaneType], Reason=[Reason])

Host Unit Link Abnormal.

Attribute

AlarmID	Alarm OID	Alarm Severity	Alarm Type
15795527	1.3.6.1.4.1.2011.5.25.241.6.3.9	Minor	Equipment alarm

Parameters

Name	Meaning
VMName	VM name.
VMUUID	VM UUID.
Reason	Alarm reason.

Impact on the System

- Create VM failed in cloud platform.The VM cannot work properly, affecting services deployed on the VM.
- Delete VM failed in cloud platform.Services will not be affected.
- VM exists in cloud platform but not in local.Services will not be affected.
- VM exists in local but not in cloud platform.The VM cannot work properly, affecting services deployed on the VM.

Possible Causes

- Create VM failed in cloud platform.
- Delete VM failed in cloud platform.
- VM exists in cloud platform but not in local.
- VM exists in local but not in cloud platform.

Procedure

- Create VM failed in cloud platform.
Collect log files and contact Huawei technical support.
- Delete VM failed in cloud platform.
Collect log files and contact Huawei technical support.
- VM exists in cloud platform but not in local.
Collect log files and contact Huawei technical support.
- VM exists in local but not in cloud platform.
Collect log files and contact Huawei technical support.

Related Information

None.

3.5.3 LSW Alarms

3.5.3.1 ALM-135462929 hwCommunicateError

Description

The communication channel failed.
(hwEntityPhysicalIndex=[hwEntityPhysicalIndex],
entPhysicalName=[entPhysicalName],
hwEntityTrapEntType=[hwEntityTrapEntType],
hwEntityTrapFaultID=[hwEntityTrapFaultID],
hwEntityCommunicateType=[hwEntityCommunicateType],
hwEntityTrapReasonDescr=[hwEntityTrapReasonDescr])

The control channel between physical entities is faulty.

Attribute

AlarmID	Alarm OID	Alarm Severity	Alarm Type
135462929	1.3.6.1.4.1.2011.5.25.219.2.9.1	Major	Communication alarm

Parameters

Name	Meaning
hwEntityPhysicalIndex	Physical entity index
entPhysicalName	Physical entity name
hwEntityTrapEntType	Physical Entity Type
hwEntityTrapFaultID	Fault Code
hwEntityCommunicateType	Communication Type
hwEntityTrapReasonDescr	Problem Description

Impact on the System

1. If the alarm is generated because the board is removed, the alarm has no impact on the system.
 2. In the dual-MPU environment, there are active and standby links for inter-board communication. If a link fault alarm is reported, the intra-board communication link is switched to the standby link. This does not affect services. However, the problem needs to be confirmed.
- If both links on the same board have alarms, inter-board packet loss occurs, which affects services and causes the board to reset due to heartbeat loss.

Possible Causes

- 1.Manual board reset or unplug
- 2.The control channel between MPU and the board is abnormal
3. The physical link from cpu to local switch is abnormal

Procedure

1. Check the alarm information and board registration information of the same type. Check whether the board is removed and restarted at the time when the alarm is reported. If yes, the board is restarted. The link is down because the board is removed and then installed. After the board is registered, the link is recovered.
2. If the card is not resealed or restarted and the alarm persists for a long time or is generated repeatedly when the card is running properly, the inter-card link communication is abnormal. In this case, collect alarm, log, and configuration information and contact technical support personnel.

Related Information

None.

3.5.3.2 ALM-135462997 hwEntityInvalid

Description

BASETRAP/1/ENTITYINVALID: OID [oid] Physical entity failed.
(EntityPhysicalIndex=[INTEGER], BaseTrapSeverity=[INTEGER],
BaseTrapProbableCause=[INTEGER], BaseTrapEventType=[INTEGER],
EntPhysicalContainedIn=[INTEGER], EntPhysicalName="[OCTET]",
RelativeResource="[OCTET]", ReasonDescription="[OCTET]")

The physical entity is faulty.

Attribute

AlarmID	Alarm OID	Alarm Severity	Alarm Type
135462997	1.3.6.1.4.1.2011.5. 25.129.2.1.9	Critical	Equipment alarm

Parameters

Name	Meaning
oid	Indicates the MIB object ID of the alarm.
EntityPhysicalIndex	Indicates the physical index.

Name	Meaning
BaseTrapSeverity	Indicates the alarm severity.
BaseTrapProbableCause	Indicates the possible causes of the alarm.
BaseTrapEventType	Indicates the alarm type.
EntPhysicalContainedIn	Indicates the parent index of the entity.
EntPhysicalName	Indicates the name of the entity.
RelativeResource	Indicates the part related to the alarm.
ReasonDescription	Indicates the description of the alarm cause.

Impact on the System

The problematic board does not work, and services on the board are interrupted. If a PHY failure has occurred, the RUN indicator on the board is off, and the Alarm indicator is steady red.

Possible Causes

Cause 1:

Optical modules used on the board are non-Huawei-certified switch optical modules. This alarm may also be reported for early delivered Huawei optical modules because vendor information of these optical modules is not recorded.

Cause 2:

The link between the CPU and PCI bridge has failed. (PCI stands for Peripheral Component Interconnect.)

Cause 3:

The link between the CPU and forwarding module has failed.

Cause 4:

The field programmable gate array (FPGA) does not work normally.

Cause 5:

The network processor (NP) does not work normally.

Cause 6:

The phase-locked loop (PLL) is abnormal.

Cause 7:

The complex programmable logical device (CPLD) does not work normally.

Cause 8:

The link between the CPU and PCI-PCIe bridge has failed. (PCIe stands for Peripheral Component Interconnect Express.)

Cause 9:

Physical ports on the chip do not work normally.

Cause 10:

Fans do not work normally.

Cause 11:

The Centralized Monitoring Unit (CMU) of the switch does not work normally.

Cause 12:

An error occurs when operations are performed on the flash memory.

Cause 13:

The PHY layer does not work normally.

Cause 14:

The TCAM does not work normally.

Cause 15:

The RTC does not work normally.

Procedure

- Rectify the fault based on the error code.

Error Code	Possible Causes and Impact on the System	Procedure
1326 10	The CMU does not match the device model, so the CMU does not work and the power supply units and fans may run abnormally.	1. Run the display device command to check device model information. 2. Use a CMU that matches the device model. For the mappings between CMUs and device models, see the Hardware Query Tool .
1326 13	The serial gigabit media independent interface (SGMII) channel between the CPU and field programmable gate array (FPGA) on the card has failed. Packets cannot be sent to the CPU for processing.	Restart the faulty card and check whether the alarm persists. If the alarm is not cleared, replace the faulty card in the slot.

Error Code	Possible Causes and Impact on the System	Procedure
1326 25	The chip on the card has failed. If an LPU fails, all services running on the LPU may be interrupted. If the standby MPU fails, the system reliability will be affected. If the active MPU fails, an active/standby switchover will occur.	Restart the faulty card and check whether the alarm persists. If the alarm is not cleared, replace the faulty card in the slot.
1326 27	The card fails to register.	Restart the faulty card and check whether the alarm persists. If the alarm is not cleared, replace the faulty card in the slot.
	Run the power off slot <i>slot-id</i> command to power off the faulty card.	Check whether the operation is required by services. • If so, this alarm is informational and no action is required. • If not and the card is still required, run the power on slot <i>slot-id</i> command to power on the card.
	Run the reset slot <i>slot-id</i> command to reset the card.	This alarm is informational and no action is required.
1326 32	The Peripheral Component Interconnect (PCI) bus failed.	Restart the faulty card and check whether the alarm persists. If the alarm is not cleared, replace the faulty card in the slot.
1326 48	After you hold down the OFL button on the faulty card for 6 seconds, the card becomes unavailable and this alarm is generated. Services are not affected.	Wait until the OFL indicator on the card turns red, and then remove the card. If the card is not removed within 10 minutes, the card will be reset and go online again.

Related Information

None.

3.5.3.3 ALM-135462998 hwCardFail

Description

ENTITYTRAP/2/CARDFAIL: OID [oid] Card fails. (Index=[INTEGER], EntityPhysicalIndex=[INTEGER], PhysicalName="[OCTET]", EntityTrapEntType=[INTEGER], EntityTrapFaultID=[INTEGER])

Some functions on a card fail.

Attribute

AlarmID	Alarm OID	Alarm Severity	Alarm Type
135462998	1.3.6.1.4.1.2011.5.25.219.2.3.3	Critical	Equipment alarm

Parameters

Name	Meaning
oid	Indicates the MIB object ID of the alarm.
Index	Indicates the alarm index.
EntityPhysicalIndex	Indicates the physical entity index.
PhysicalName	Indicates the name of the physical entity where the alarm is generated.
EntityTrapEntType	Indicates the alarm type.
EntityTrapFaultID	Indicates the error code of the alarm, which is 135194.

Impact on the System

The IIC bus cannot be accessed normally.

Possible Causes

The IIC bus has failed.

Procedure

- Remove and install the card and then check whether the alarm is cleared.
 - If so, the alarm handling ends.
 - If not, go to step 2.
- Replace the card and check whether the alarm is cleared.

- If so, the alarm handling ends.
- If not, collect alarm information and configuration information, and then contact technical support personnel.

Related Information

None.

3.5.3.4 ALM-135462999 hwCardInvalid

Description

ENTITYTRAP/1/CARDINVALID: OID [oid] Card is invalid for some reason.
(Index=[INTEGER], EntityPhysicalIndex=[INTEGER], PhysicalName="[OCTET]",
EntityTrapEntType=[INTEGER], EntityTrapFaultID=[INTEGER],
EntityTrapReasonDescr="[OCTET]")

The subcard does not work.

Attribute

AlarmID	Alarm OID	Alarm Severity	Alarm Type
135462999	1.3.6.1.4.1.2011.5.25 .219.2.3.5	Critical	Equipment alarm

Parameters

Name	Meaning
oid	Indicates the MIB object ID of the alarm.
Index	Indicates the alarm ID.
EntityPhysicalIndex	Indicates the index.
PhysicalName	Indicates the physical entity name.
EntityTrapEntType	Indicates the alarm type.
EntityTrapFaultID	Indicates the error code.
EntityTrapReasonDescr	Indicates the description of the alarm cause.

Impact on the System

The IIC bus cannot be accessed normally.

Possible Causes

The IIC bus has failed.

Procedure

- Remove and install the card and then check whether the alarm is cleared.
 - If so, the alarm handling ends.
 - If not, go to step 2.
- Replace the card and check whether the alarm is cleared.
 - If so, the alarm handling ends.
 - If not, collect alarm information and configuration information, and then contact technical support personnel.

Related Information

None.

3.5.3.5 ALM-134292070 hwPoePowerOff

Description

PD powered off. (IfIndex=[IfIndex], Interface=[Interface], FaultID=[FaultID])

PD powered off.

Attribute

AlarmID	Alarm OID	Alarm Severity	Alarm Type
134292070	1.3.6.1.4.1.2011.5.25 .195.40.2	Warning	Equipment alarm

Parameters

Name	Meaning
IfIndex	Indicates the index of the faulty interface.
Interface	Indicates the faulty interface name.
FaultID	Error code.

Impact on the System

The PD connected to the interface is powered off and cannot work normally.

Possible Causes

1. The PD is removed.
2. The PD is faulty.
3. When the power is insufficient, the interface with a higher priority preempts the power.
4. The interface to which the PD connects is automatically powered off in the power-off time range.
5. The PD is powered off because of overcurrent protection.

Procedure

1. Check whether the PD is removed.
If so, go to step 2.
If not, go to step 4.
2. Check whether the PD is removed because of a normal operation.
If so, the alarm handling ends.
If not, go to step 3.
3. Install the PD to check whether it is powered on.
If so, the alarm handling ends.
If not, go to step 4.
4. Run the **display poe power-state** *interface-type interface-number* command to check whether the maximum output power of the interface is sufficient.
If so, go to step 5.
If not, connect the PD to another interface or PoE device.
5. Run the **display poe power-state** *interface-type interface-number* command to check whether the power supply priority of the interface is low.
If so, go to step 6.
If not, go to step 8.
6. Check whether the power supply priority of the interface needs to be reconfigured.
If so, go to step 6.
If not, go to step 7.
7. Run the **poe priority** command to configure the power supply priority of the interface. Then check whether the PD is powered on.
If so, the alarm handling ends.
If not, go to step 8.
8. Run the **display poe power-state** *interface-type interface-number* command to check whether the interface is in the power-off time range.
If so, the alarm handling ends.
If not, go to step 9.
9. Check whether the PD is faulty.
If so, replace it.

If not, collect alarm information and configuration information, and then contact technical support personnel.

Related Information

None.

3.5.3.6 ALM-134292071 hwPoePdConnected

Description

PD connected. (IfIndex=[IfIndex], Interface=[Interface])

PD connected.

Attribute

AlarmID	Alarm OID	Alarm Severity	Alarm Type
134292071	1.3.6.1.4.1.2011.5.25 .195.40.8	Warning	Equipment alarm

Parameters

Name	Meaning
IfIndex	Indicates the index of the faulty port.
Interface	Indicates the faulty port name.

Impact on the System

In normal cases, the system starts feeding power to the PD.

Possible Causes

The system detects a valid PD.

Procedure

This alarm message is informational only, and no action is required.

Related Information

None.

3.5.3.7 ALM-134292072 hwPoePdDisconnected

Description

PD disconnected. (IfIndex=[IfIndex], Interface=[Interface])

PD disconnected.

Attribute

AlarmID	Alarm OID	Alarm Severity	Alarm Type
134292072	1.3.6.1.4.1.2011.5.25 .195.40.9	Warning	Equipment alarm

Parameters

Name	Meaning
IfIndex	Indicates the index of the faulty port.
Interface	Indicates the faulty port name.

Impact on the System

The system stops feeding power to the PD.

Possible Causes

A valid PD is removed.

Procedure

1. Reinstall the PD. Then check whether the fault is cleared.
 - If so, go to Step 3.
 - If not, go to Step 2.
2. Collect the trap information, log information, and configuration information, and then contact technical personnel.
3. End.

Related Information

None.

3.5.3.8 ALM-15795217 hwPoePdClassInvalid

Description

PD with invalid IEEE class and power denied. (IfIndex=[IfIndex], Interface=[Interface])

The system detects that the PD class is invalid.

Attribute

AlarmID	Alarm OID	Alarm Severity	Alarm Type
15795217	1.3.6.1.4.1.2011.5.25.195.40.10	Warning	Equipment alarm

Parameters

Name	Meaning
IfIndex	Interface index
Interface	Interface name

Impact on the System

Services are not affected.

Possible Causes

Cause 1:

The PD may not comply with standards, whereas the switch supports 802.3af and 802.3at. In this case, the PD class cannot be identified by the switch.

Cause 2:

The PD hardware is faulty.

Cause 3:

The PoE chip of the device is faulty.

Procedure

1. Run the **poe legacy enable** command on the interface to enable compatibility detection and then check whether the alarm is cleared.
If so, the alarm handling ends.
If not, go to step 2.
2. Replace the PD with a standard PD and then check whether the alarm is cleared.

If so, the alarm handling ends.

If not, collect alarm information and configuration information, and then contact technical support personnel.

Related Information

None.

3.5.3.9 ALM-15795218 hwPoePdPriorityDifferent

Description

The priority of interface and PD is inconsistent. (IfIndex=[IfIndex], Interface=[Interface], PortPriority=[PortPriority], PDPriority=[PDPriority])

The interface priority is different from the PD priority.

Attribute

AlarmID	Alarm OID	Alarm Severity	Alarm Type
15795218	1.3.6.1.4.1.2011.5.25.195.40.16	Warning	Equipment alarm

Parameters

Name	Meaning
IfIndex	Interface index
Interface	Interface name
PortPriority	Interface priority
PDPriority	PD priority

Impact on the System

Services are not affected.

Possible Causes

The interface priority is low, whereas the PD priority is high.

Procedure

1. Run the **poe priority** command to change the interface priority to be higher than the PD priority.

Related Information

None.

3.5.3.10 ALM-15795219 hwPoePowerOverUtilizationThreshold

Description

POE/4/PWRUTITHRESH: OID [oid] PSE power consumption has exceeded the upper limit. (ChassisID=[INTEGER], ConsumingPower=[INTEGER], PowerThreshold=[INTEGER])

PSE power consumption has exceeded the upper limit.

Attribute

AlarmID	Alarm OID	Alarm Severity	Alarm Type
15795219	1.3.6.1.4.1.2011.5.25.195.40.17	Warning	Equipment alarm

Parameters

Name	Meaning
DeviceID	Indicates the device ID.
ConsumingPower	Indicates the current power consumption.
PowerThreshold	Indicates the power threshold.

Impact on the System

If the alarm persists, all the PDs may be powered off because of insufficient power supply.

Possible Causes

The total power consumption of all the PDs is greater than or equal to the alarm threshold.

Procedure

1. Check whether the power consumption of the PDs is within the accepted range.
 - If so, go to step 2.
 - If not, go to step 3.

2. Run the **poe-power utilization-threshold** command to change the alarm threshold for PoE power consumption percentage.
3. Replan the network based on the system external power supply capability. Run the **poe priority** command to increase the priority of important PDs to prevent their power from being occupied by other PDs. Power off the PDs that are not required to ensure system reliability.

Related Information

None.

3.5.3.11 ALM-15795325 hwPoePowerOn

Description

PD powered on. (IfIndex=[IfIndex], Interface=[Interface])

PD powered on.

Attribute

AlarmID	Alarm OID	Alarm Severity	Alarm Type
15795325	1.3.6.1.4.1.2011.5.25 .195.40.3	Warning	Equipment alarm

Parameters

Name	Meaning
IfIndex	Indicates the index of the interface.
Interface	Indicates the interface name.

Impact on the System

Services are not affected.

Possible Causes

The device starts to properly supply power.

Procedure

This trap message is informational only, and no action is required.

Related Information

None.

3.5.3.12 ALM-15795346 hwPoePdClassOvercurrent

Description

POE/4/PDCLASSOVERCURRENT: OID [oid] has detected an overcurrent PD in classification and power denied. (IfIndex=[INTEGER], Interface="[OCTET]")

Port has detected a classification overcurrent PD and power denied.

Attribute

AlarmID	Alarm OID	Alarm Severity	Alarm Type
15795346	1.3.6.1.4.1.2011.5.25.195.40.11	Warning	Equipment alarm

Parameters

Name	Meaning
IfIndex	Indicates the index of the faulty port.
Interface	Indicates the faulty port name.

Impact on the System

Services are not affected.

Possible Causes

Cause 1:

The PD may not comply with standards, whereas the switch supports 802.3af and 802.3at. In this case, the PD class cannot be identified by the switch.

Cause 2:

The PD hardware is faulty.

Cause 3:

The PoE chip of the device is faulty.

Procedure

1. Run the **poe high-inrush enable slot** *slot-id* command in the system view to allow high inrush current during power-on and then check whether the alarm is cleared.
If so, the alarm handling ends.
If not, go to step 2.

2. Replace the PD with a standard PD and then check whether the alarm is cleared.
If so, the alarm handling ends.
If not, collect alarm information and configuration information, and then contact technical support personnel.

Related Information

None.

3.5.3.13 ALM-223617026 hwMstpProRootLost

Description

The bridge loses the position of root bridge.(ProcessID=[ProcessID], InstanceID=[InstanceID], ProInstRootType=[ProInstRootType])
A device lost its root bridge role.

Attribute

AlarmID	Alarm OID	Alarm Severity	Alarm Type
223617026	1.3.6.1.4.1.2011.5.25.42.4.2.28	Major	Communication alarm

Parameters

Name	Meaning
ProcessID	MSTP process ID
InstanceID	Instance ID
ProInstRootType	Root bridge role type

Impact on the System

Services may be interrupted.

Possible Causes

- Cause 1: The bridge ID of new equipment is not optimal.
- Cause 2: Modify thr priority or domain configuration of the device in the original network.

Procedure

- Cause 1: The bridge ID of new equipment is not optimal.
 - a. Check whether the added physical link is the required one.
 - If the physical link is required, go to Step 2.
 - If the physical link is not required, go to Step 3.
 - b. Run the `display stp [ process process-id ] [ instance instance-id ] [ interface interface-type interface-number | slot slot-id | vsi vsi-name pw pw-name ] [ brief ]` command on the newly added device to check whether the bridge ID is optimal on the entire network.
 - If the bridge ID is optimal on the entire network, go to Step 3.
 - If the bridge ID is not optimal on the entire network, go to Step 5.
 - c. Check whether the bridge ID of the newly added device should be planned as the optimal ID on the entire network.
 - If the bridge ID should be planned as the optimal one on the entire network, no action is required.
 - If the bridge ID should not be planned as the optimal one on the entire network, go to Step 4.
 - d. Perform configuration correctly based on the network topology and check whether the alarm is cleared. If the alarm persists, go to Step 5.
 - e. Collect alarm and configuration information, and contact technical support personnel.
- Cause 2: Modify the priority or domain configuration of the device in the original network.
 - a. Run the `display stp [ process process-id ] [ instance instance-id ] [ interface interface-type interface-number | slot slot-id | vsi vsi-name pw pw-name ] [ brief ]` command to check whether the instance's priority vector or region configuration change is normal.
 - If yes, no action is required.
 - If not, go to Step 2.
 - b. Perform configuration correctly based on the network topology. If the alarm persists, go to Step 3.
 - c. Collect alarm information and configuration information, and then contact technical support personnel.

Related Information

None.

3.5.3.14 ALM-15794194 hwGtlResourceUsedUp

Description

GTL/2/RESOURCE_USEDUP:OID [OID] Resource item [item-name] is nearly used up.

The trap was generated when the percentage of the resources used by the service module was not less than the 90% which is defined by the license.

Attribute

AlarmID	Alarm OID	Alarm Severity	Alarm Type
15794194	1.3.6.1.4.1.2011.5.25 .142.2.2	Major	Quality of service alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
item-name	Indicates the name of the resource item.

Impact on the System

Under the control of the license, the usage percentage of service resources cannot exceed the threshold defined by the license. Therefore, if a larger license file cannot be applied for or activated, traffic loads cannot cater for the demand of the current operation scenario.

NOTE

This trap is reported only once when the percentage of resources used by the service module reaches or exceeds 90% of the threshold defined by the license.

Possible Causes

The usage of an active resource item (not an interface resource item) in the license file exceeded the upper threshold.

Procedure

1. Confirm whether the current license file is large enough. If not, apply for a larger license file.
2. Use the new license file and run the **license active** *license-name* command to activate it.

3. Collect alarm information and configuration information, and then contact technical support personnel.

Related Information

None.

3.5.3.15 ALM-157163598 hwMflpBdAlarm

Description

MAC flapping detected, BdlId = [BdlId], Original-Port = [IfNameA], Flapping port 1 = [IfNameB], port 2 = [IfNameC]. [AlarmReason].

MAC address flapping occurs in the BD.

Attribute

AlarmID	Alarm OID	Alarm Severity	Alarm Type
157163598	1.3.6.1.4.1.2011.5.25 .160.3.17	Warning	Quality of service alarm

Parameters

Name	Meaning
BdlId	BD ID.
IfNameA	Port before MAC address flapping.
IfNameB	Port 1 after MAC address flapping.
IfNameC	Port 2 after MAC address flapping.
AlarmReason	Description of the alarm cause.

Impact on the System

Traffic cannot be forwarded.

Possible Causes

There may be loops on the current network.

Procedure

- Configure the interface to enter the error-down state when MAC address flapping occurs on the interface or eliminate loops on the network.

Related Information

None.

3.5.3.16 ALM-161611792 hwStackLogicStackPortLinkErr

Description

The interface Stack-Port was linked invalidly.
(hwStackLocalIfName=[hwStackLocalIfName],
hwStackPeerIfName=[hwStackPeerIfName], Reason=[Reason])

Physical member ports of the stack port were connected incorrectly.

Attribute

AlarmID	Alarm OID	Alarm Severity	Alarm Type
161611792	1.3.6.1.4.1.2011.5.25 .183.1.22.9	Critical	Environmental alarm

Parameters

Name	Meaning
hwStackLocalIfName	Indicates the name of the local stack port.
hwStackPeerIfName	Indicates the name of the peer stack port.
Reason	Indicates a possible cause.

Impact on the System

- The CSS or stack cannot be set up. CSS or stack members are removed, and the CSS or stack split.
- The Stack-Port on the local device receives packets from different Stack-Ports on the peer device.
- The Stack-Port on the local device receives packets from different devices.
- The Stack-Port on the local device receives packets from the Stack-Ports on different LPUs of the peer device.
- A CSS or stack cannot be set up.

Possible Causes

- Cause 1: The Stack-Ports have loop connections.
- Cause 2: A Stack-Port on the local device is connected to two different Stack-Ports on the peer device.

- Cause 3: A Stack-Port on the local device is connected to Stack-Ports on different devices.
- Cause 4: A Stack-Port on an LPU of the local device is connected to the Stack-Ports on different LPUs of the peer device.
- Cause 5: The physical port is connected to the device with a conflicting ID.

Procedure

- Cause 1: The Stack-Ports have loop connections.
 - a. Run the **display interface brief** command to check the member ports in a Stack-Port. Determine whether any two ports in the same Stack-Port are connected.
 - If so, disconnect the ports.
 - If not, go to step 2.
 - b. Check whether the member ports in a Stack-Port are connected to different devices.
 - If so, check the protocol status of these ports. Remove the cables that connect the ports whose physical status is Up but protocol status is Down.
 - If not, go to step 3.
 - c. Check whether the member ports in a Stack-Port are connected to another Stack-Port on the same device.
 - If so, run the **display css topology** or **display stack topology** command to check the CSS or stack ID of the device that the Stack-Port is connected to. Remove the cables that connect the ports to another device.
 - If not, go to step 4.
 - d. Collect traps, logs, and configurations, and contact technical support personnel.
- Cause 2: A Stack-Port on the local device is connected to two different Stack-Ports on the peer device.

Ensure one-to-one connections for Stack-Ports.
- Cause 3: A Stack-Port on the local device is connected to Stack-Ports on different devices.

Ensure one-to-one connections for Stack-Ports.
- Cause 4: A Stack-Port on an LPU of the local device is connected to the Stack-Ports on different LPUs of the peer device.

Remove the cross-connect cable.
- Cause 5: The physical port is connected to the device with a conflicting ID.

Ensure that the stack IDs at the two ends of the connection are different.

Related Information

None.

3.5.3.17 ALM-157024263 hwGtlItemmismatch

Description

The license item of slot [hwGtlChassisID] mismatched with the main board.

The license control item or serial number of the specified chassis is inconsistent with that of the main control chassis.

Attribute

AlarmID	Alarm OID	Alarm Severity	Alarm Type
157024263	1.3.6.1.4.1.2011.5.25 .142.2.6	Minor	Quality of service alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
hwGtlChassisID	Indicates the description of the ID of the current shelf or board.

Impact on the System

Services will not be affected.

Possible Causes

The license item or serial number of the chassis mismatched with that of the main chassis.

Procedure

Apply for a license file that matches the main control frame

Related Information

None.

3.5.3.18 ALM-157155346 hwMflpVlanLoopAlarm

Description

MAC flapping detected, VlanId = [VlanId], Original-Port = [IfNameA], Flapping port 1 = [IfNameB], port 2 = [IfNameC]. [AlarmReason].

MAC address flapping occurs in a VLAN.

Attribute

AlarmID	Alarm OID	Alarm Severity	Alarm Type
157155346	1.3.6.1.4.1.2011.5.25 .160.3.13	Warning	Quality of service alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
VlanId	VLAN ID.
IfNameA	Drift source port.
IfNameB	Destination port of the floating IP address.
IfNameC	Destination port of the floating IP address.
AlarmReason	Alarm cause.

Impact on the System

Traffic cannot be forwarded.

Possible Causes

There may be loops on the current network.

Procedure

Configure the error-down function on the interface or eliminate loops on the network.

Related Information

None.

3.5.3.19 ALM-157163596 hwBdMacLimitOverThresholdAlarm

Description

MAC address learning reached the limit. (Bd=[BdId],
MacLimitMaxMac=[MacLimitMaxMac].)

The number of learned MAC addresses reached the alarm threshold.

Attribute

AlarmID	Alarm OID	Alarm Severity	Alarm Type
157163596	1.3.6.1.4.1.2011.5.25 .42.2.1.7.36	Warning	Quality of service alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
BdId	BD ID.
MacLimitMaxMac	Maximum number of MAC addresses that can be learned.

Impact on the System

When the number of learned MAC address entries reaches the limit, the device no longer learns new MAC address entries.

Possible Causes

The number of learned dynamic MAC addresses exceeded the maximum size of the MAC address table.

Procedure

- This is a normal prompt and no action is required.

Related Information

None.

3.5.3.20 ALM-157163635 hwVxlanTunnelMacLimitOverThresholdAlarm

Description

MAC address learning reached the limit. (SourceIpAddress=[SourceIp], DestinationIpAddress=[PeerIp], MacLimitMaxMac=[MacLimitMaxMac].)

This object indicates that the number of MAC addresses learned by a VXLAN tunnel reaches the upper alarm threshold.

Attribute

AlarmID	Alarm OID	Alarm Severity	Alarm Type
157163635	1.3.6.1.4.1.2011.5.25.42.2.1.7.63	Warning	Quality of service alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
SourceIp	Source IP address of a tunnel.
PeerIp	Peer IP address of a tunnel.
MacLimitMaxMac	Maximum number of MAC addresses that can be learned.

Impact on the System

When the number of learned MAC address entries reaches the limit, the device no longer learns new MAC address entries.

Possible Causes

The number of learned dynamic MAC addresses exceeded the maximum size of the MAC address table.

Procedure

1. Delete unnecessary MAC addresses or run the peer ip-address mac-address limit maximum max command to increase the maximum number of MAC addresses that can be learned.

Related Information

None.

3.5.3.21 ALM-257564679 hwVlanMacLimitOverThreshold

Description

MAC address learning reached the limit.
(Vlan=[VlanId],MacLimitMaxMac=[MacLimitMaxMac])

The number of learned MAC addresses reached the alarm threshold.

Attribute

AlarmID	Alarm OID	Alarm Severity	Alarm Type
257564679	1.3.6.1.4.1.2011.5.25 .42.2.1.7.67	Warning	Quality of service alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
VlanId	VLAN ID.
MacLimitMaxMac	Maximum number of MAC addresses that can be learned.

Impact on the System

When the number of learned MAC address entries reaches the limit, the device no longer learns new MAC address entries.

Possible Causes

The number of learned dynamic MAC addresses exceeded the maximum size of the MAC address table.

Procedure

Delete unnecessary MAC addresses or run the **mac-address limit** command in the VLAN view to increase the limit.

Related Information

None.

3.5.3.22 ALM-257564680 hwPortMacLimitOverThreshold

Description

MAC address learning reached the limit.
(Vlan=[VlanId],MacLimitMaxMac=[MacLimitMaxMac])

The number of learned MAC addresses reached the alarm threshold.

Attribute

AlarmID	Alarm OID	Alarm Severity	Alarm Type
257564680	1.3.6.1.4.1.2011.5.25 .42.2.1.7.69	Warning	Quality of service alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
L2IfPortName	Name of an interface.
MacLimitMaxMac	Maximum number of MAC addresses that can be learned.

Impact on the System

When the number of learned MAC address entries reaches the limit, the device no longer learns new MAC address entries.

Possible Causes

The number of learned dynamic MAC addresses exceeded the maximum size of the MAC address table.

Procedure

Delete unnecessary MAC addresses or run the **mac-address limit** command in the VLAN view to increase the limit.

Related Information

None.

3.5.3.23 ALM-157163553 hwMacUsageRaisingInfo

Description

MAC usage reached the Threshold. (PhysicalName=[entPhysicalName],
MacEntityUsage=[hwMacEntityUsage],
MacEntityUsageThreshold=[hwMacEntityUsageThreshold].)

The MAC address table usage exceeded the threshold.

Attribute

AlarmID	Alarm OID	Alarm Severity	Alarm Type
157163553	1.3.6.1.4.1.2011.5.25 .42.2.1.7.1	Warning	Quality of service alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
entPhysicalName	NE Name
hwMacEntityUsage	MAC table usage
hwMacEntityUsageThreshold	Alarm threshold for MAC address table usage

Impact on the System

After the MAC address usage reaches the alarm threshold, some MAC addresses may fail to be learned.

Possible Causes

The MAC address table usage reaches 80% of the threshold.

Procedure

- Delete unnecessary static MAC address entries. See **mac-address static vlan**.

Related Information

None.

3.5.3.24 ALM-234102790 hwMacMovedQuietMaxUserAlarm

Description

The number of mac moved quiet users reached the maximum.
(SpecOfUserNum=[SpecOfUserNum],CurrentThreshold=[CurrentThreshold]%,LowerThreshold=[LowerThreshold]%,UpperThreshold=[UpperThreshold]%,ProcessName=[ProcessName])
The percentage of current MAC address migration users in quiet state against the maximum number of users exceeds the upper alarm threshold.

Attribute

Alarm ID	OID	Alarm Severity	Alarm Type
234102790	1.3.6.1.4.1.2011.5.2.2.2.0.53	Warning	Quality of service alarm

Parameters

Name	Meaning
SpecOfUserNum	Indicates the maximum number of MAC address migration users in quiet state.
CurrentThreshold	Indicates the percentage of MAC address migration users in quiet state against the maximum number of users.
LowerThreshold	Indicates the lower alarm threshold for the percentage of MAC address migration users in quiet state against the maximum number of users.
UpperThreshold	Indicates the upper alarm threshold for the percentage of MAC address migration users in quiet state against the maximum number of users.
ProcessName	Process Name.

Impact on the System

None

Possible Causes

The percentage of current MAC address migration users in quiet state against the maximum number of users exceeds the upper alarm threshold.

Procedure

- 1.Run the **display authentication mac-move configuration** command in any view to check whether the upper threshold of MAC address migration users in quiet state is set.
 - If it is configured, consider whether to delete it.
 - If it is not configured, adjust the network based on the number of access users. If the problem persists, go to 2.
2. Collect log information and contact technical support personnel.

3.5.3.25 ALM-234102791 hwMacMovedQuietUserClearAlarm

Description

The MAC Moved Quiet Max User Alarm is cleared.
(SpecOfUserNum=[SpecOfUserNum],CurrentThreshold=[CurrentThreshold]%,LowerThreshold=[LowerThreshold]%,UpperThreshold=[UpperThreshold]%,ProcessName=[ProcessName])

The percentage of current MAC address migration users in quiet state against the maximum number of users decreases to be equal to or smaller than the lower alarm threshold.

Attribute

Alarm ID	OID	Alarm Severity	Alarm Type
234102791	1.3.6.1.4.1.2011.5 .2.2.2.0.54	Warning	Quality of service alarm

Parameters

Name	Meaning
SpecOfUserNum	Indicates the maximum number of MAC address migration users in quiet state.
CurrentThreshold	Indicates the percentage of MAC address migration users in quiet state against the maximum number of users.

Name	Meaning
LowerThreshold	Indicates the lower alarm threshold for the percentage of MAC address migration users in quiet state against the maximum number of users.
UpperThreshold	Indicates the upper alarm threshold for the percentage of MAC address migration users in quiet state against the maximum number of users.
ProcessName	Process Name.

Impact on the System

The clear alarm generated when the percentage of MAC address migration users in quiet state reaches the upper threshold has no impact on the system.

Possible Causes

The percentage of current MAC address migration users in quiet state against the maximum number of users decreases to be equal to or smaller than the lower alarm threshold.

Procedure

Collect log information and contact technical support personnel.

3.5.3.26 ALM-233578498 hwMacQuietMaxUserAlarm

Description

The number of mac quiet users reached the maximum. (Spec of User Num=[SpecofUserNum], Current Threshold=[CurrentThreshold], Lower Threshold=[LowerThreshold], Upper Threshold=[UpperThreshold], Process Name=[ProcessName])

The number of MAC address authentication users in quiet state reached the maximum value.

Attribute

Alarm ID	OID	Alarm Severity	Alarm Type
233578498	1.3.6.1.4.1.2011.5.2.2.2.0.118	Warning	Quality of service alarm

Parameters

Name	Meaning
SpecofUserNum	Indicates the spec of user num.
CurrentThreshold	Indicates the current threshold.
LowerThreshold	Indicates the lower alarm threshold for the percentage of users in quiet state.
UpperThreshold	Indicates the upper alarm threshold for the percentage of users in quiet state.
ProcessName	Process name.

Impact on the System

None

Possible Causes

The percentage of current MAC address authentication users in quiet state to the total MAC address authentication users in quiet state exceeded the upper alarm threshold.

Procedure

Collect log information and contact technical support.

3.5.3.27 ALM-233578499 hwMacQuietUserClearAlarm

Description

The MAC Quiet Max User Alarm is cleared. (Spec of User Num=[SpecofUserNum],Current Threshold=[CurrentThreshold],Lower Threshold=[LowerThreshold],Upper Threshold=[UpperThreshold],Process Name=[ProcessName])

The alarm indicating that the number of MAC address authentication users in quiet state reached the maximum value is cleared.

Attribute

Alarm ID	OID	Alarm Severity	Alarm Type
233578499	1.3.6.1.4.1.2011.5.2.2.2.0.119	Warning	Quality of service alarm

Parameters

Name	Meaning
SpecofUserNum	Indicates the spec of user num.
CurrentThreshold	Indicates the current threshold.
LowerThreshold	Indicates the lower alarm threshold for the percentage of users in quiet state.
UpperThreshold	Indicates the upper alarm threshold for the percentage of users in quiet state.
ProcessName	Process name.

Impact on the System

None

Possible Causes

The percentage of current MAC address authentication users in quiet state to the total MAC address authentication users in quiet state fell equal to or below the lower alarm threshold.

Procedure

This alarm is informational only, and no action is required.

3.5.3.28 ALM-233574400 hwnACMaxUserAlarm

Description

The number of NAC users reached the maximum. (Slot=[Slot],User-num=[User-num],Threshold=[Threshold]%)

The percentage of successfully authenticated NAC users reached the upper alarm threshold.

Attribute

Alarm ID	OID	Alarm Severity	Alarm Type
233574400	1.3.6.1.4.1.2011.5.2.2.2.0.107	Warning	Quality of service alarm

Parameters

Name	Meaning
Slot	Slot ID.
User-num	Current user Num.
Threshold	Indicates the percentage of NAC users against the spec of users.
ProcessName	Process name.

Impact on the System

None

Possible Causes

The percentage of successfully authenticated NAC users reached the upper alarm threshold.

Procedure

1. Run the **display authentication user-alarm configuration** command in any view to check the upper alarm threshold for the percentage of successfully authenticated NAC users. Adjust the threshold according to the network requirements. If the fault persists, go to 2.
2. Collect log information and contact technical support personnel.

3.5.3.29 ALM-234102786 hwMaxUclGroupIpNumAlarm

Description

The number of dynamic ucl-group IPs is reaching the max.
(CurrentNum=[CurrentNum], Threshold=[Threshold]%,
ProcessName=[ProcessName])

The number of dynamic UCL group IPs reached the maximum value.

Attribute

Alarm ID	OID	Alarm Severity	Alarm Type
234102786	1.3.6.1.4.1.2011.5 .2.2.2.0.124	Warning	Quality of service alarm

Parameters

Name	Meaning
CurrentNum	Indicates the current number of ucl-group ips.
Threshold	Indicates the percentage of ucl-group ips against the spec.
ProcessName	Process Name.

Impact on the System

None

Possible Causes

The number of UCL-group IPs reached the upper alarm threshold.

Procedure

1. Run the **display ucl-group all** command to check whether the number of UCL-group IPs exceeds the upper threshold.
 - If so, plan UCL groups properly.
 - If not, no action is required.
2. If the fault persists, contact technical support.

3.5.3.30 ALM-233447431 hwMacAuthenMaxUserAlarm

Description

The number of users has reached the max number. (ifIndex=[ifIndex], PortName=[PortName], Process Name=[ProcessName])

The number of MAC address authentication users reaches the upper limit.

Attribute

Alarm ID	OID	Alarm Severity	Alarm Type
233447431	1.3.6.1.4.1.2011.5.25.171.2.1	Warning	Quality of service alarm

Parameters

Name	Meaning
ifIndex	Interface index.
PortName	Port name.
ProcessName	Process name.

Impact on the System

Users cannot access through this interface.

Possible Causes

The number of MAC address authentication users reaches the upper limit

Procedure

1. Run the **display access-user interface** command to check whether online MAC address authentication users are proper.
 - If so, replace the device with a higher-performance device.
 - If not, replan the network.
2. 2.Collect log information and contact technical support personnel.

3.5.3.31 ALM-233443329 hwQuietUserClearAlarm

Description

The quiet max 802.1x user alarm is cleared. (Threshold=[Threshold]%, UserNum=[UserNum], Lower Threshold=[LowerThreshold]%, Upper Threshold=[UpperThreshold]%, Process Name=[ProcessName])

The alarm indicating that the number of 802.1x users in quiet state reached the maximum was cleared.

Attribute

Alarm ID	OID	Alarm Severity	Alarm Type
233443329	1.3.6.1.4.1.2011.5 .2.2.2.0.120	Warning	Quality of service alarm

Parameters

Name	Meaning
Threshold	Indicates the percentage of current users in quiet state to the total users in quiet state.
UserNum	Indicates the number of users in quiet state.
LowerThreshold	Indicates the lower alarm threshold for the percentage of users in quiet state.
UpperThreshold	Indicates the upper alarm threshold for the percentage of users in quiet state.
ProcessName	Process Name.

Impact on the System

None

Possible Causes

The percentage of current 802.1x users in quiet state fell equal to or below the lower alarm threshold.

Procedure

This alarm is informational only, and no action is required.

3.5.3.32 ALM-233443328 hwQuietUserMaxAlarm

Description

The number of quiet 802.1x users is reaching the max. (Threshold=[Threshold]%, UserNum=[UserNum], Lower Threshold=[LowerThreshold]%, Upper Threshold=[UpperThreshold]%, Process Name=[ProcessName])

The number of 802.1x users in quiet state reached the maximum value.

Attribute

Alarm ID	OID	Alarm Severity	Alarm Type
233443328	1.3.6.1.4.1.2011.5.2.2.2.0.121	Warning	Quality of service alarm

Parameters

Name	Meaning
Threshold	Indicates the percentage of current users in quiet state to the total users in quiet state.
UserNum	Indicates the number of users in quiet state.
LowerThreshold	Indicates the lower alarm threshold for the percentage of users in quiet state.
UpperThreshold	Indicates the upper alarm threshold for the percentage of users in quiet state.
ProcessName	Process Name.

Impact on the System

None

Possible Causes

The number of 802.1x users in quiet state reached the upper alarm threshold.

Procedure

1. Check whether the number of 802.1x users in quiet state exceeded the maximum value.
 - If so, check whether a large number of users who do not meet authentication requirements request authentication on the network. If such users exist, replan the network.
 - If not, no action is required.
2. If the fault persists, contact technical support.

3.5.3.33 ALM-233447430 hwSrvcfgEapMaxUserAlarm

Description

The number of users has reached the max number. (ifIndex=[ifIndex], PortName=[PortName], Process Name=[ProcessName])

The number of 802.1X authentication users reaches the upper limit.

Attribute

Alarm ID	OID	Alarm Severity	Alarm Type
233447430	1.3.6.1.4.1.2011.5 .25.40.4.2.1	Warning	Quality of service alarm

Parameters

Name	Meaning
ifIndex	Interface index.
PortName	Port name.
ProcessName	Process name.

Impact on the System

Users cannot access through this interface.

Possible Causes

The number of 802.1X authentication users reaches the upper limit.

Procedure

- 1.Run the **display access-user interface interface-type interface-number** command to check whether online 802.1X authentication users are proper.
 - If so, replace the device with a higher-performance device.
 - If not, replan the network.
2. 2.Collect log information and contact technical support personnel.

3.5.3.34 ALM-233574401 hwNACUserClearAlarm

Description

The NAC Max User Alarm is cleared. (Slot=[Slot], User-num=[User-num], Threshold=[Threshold]%)

The percentage of successfully authenticated NAC users reached or fell below the lower alarm threshold.

Attribute

Alarm ID	OID	Alarm Severity	Alarm Type
233574401	1.3.6.1.4.1.2011.5 .2.2.2.0.106	Warning	Quality of service alarm

Parameters

Name	Meaning
Slot	Slot ID.
User-num	Current user Num.
Threshold	Indicates the percentage of NAC users against the spec of users.
ProcessName	Process name.

Impact on the System

This is the clear alarm for the alarm generated when the percentage of successfully authenticated NAC users reaches the upper alarm threshold.

Possible Causes

The percentage of successfully authenticated NAC users reached or fell below the lower alarm threshold.

Procedure

This alarm is informational only, and no action is required.

3.5.3.35 ALM-15795094 SRV6_LOCAL_SID_ROUTE_CONFLICT

Description

Conflict between an SRv6 local SID and a route. (SID=[LocalSID]/[PrefixLength])
An SRv6 local SID conflicts with a route.

Attribute

Alarm ID	OID	Alarm Severity	Alarm Type
15795094	1.3.6.1.4.1.2011.5 .25.363.2.1	Warning	Communication alarm

Parameters

Parameter	Description
LocalSID	Local SID.

Parameter	Description
PrefixLength	Mask length of local SID.

Impact on the System

The routing table or SRv6 local SID table may be deleted.

Possible Causes

There was a conflict between the SRv6 local SID and route.

Procedure

Check whether route and local SID configurations are proper. If not, modify route or local SID configurations.

3.5.3.36 ALM-67706900 hwRuAuthFail

Description

The authentication to the remote unit failed. (RemoteUnitEsn=[RemoteUnitEsn])

The central switch fails to authenticate the RU.

NOTE

This alarm is supported only on S5735-L-V2, S5735-S-V2, S5735I-S-V2, S5735I-L-V2, S6730-H-V2, S5732-H-V2.

Attribute

Alarm ID	OID	Alarm Severity	Alarm Type
67706900	1.3.6.1.4.1.2011.5 .25.667.2.37	major	Quality of service alarm

Parameters

Parameter	Description
RemoteUnitEsn	ESN of the RU.

Impact on the System

Configurations cannot be delivered to the RU, and the RU cannot be restarted.

Possible Causes

The default domain of the central switch is not loaded with the correct device certificate

Procedure

1. Load the correct device certificate to the default domain for the central switch. Run the **display remote-unit [connect-interface interface-type interface-number | name remote-unit-name | verbose]** command to check whether the Authen Result field of the RU is Success.
 - If so, go to Step 3.
 - If not, go to Step 2.
2. Collect trap, log, and configuration information, and contact technical support personnel.
3. End.

3.5.3.37 ALM-67699723 hwRuMngFirmwareUpdateFail

Description

The remote-unit firmware upgrade failed. (RemoteUnitEsn=[RemoteUnitEsn], InterfaceName=[InterfaceName], Firmware=[Firmware], Reason=[Reason])

An RU fails to be upgraded.



NOTE

This alarm is supported only on S5735I-L-V2, S6730-H-V2, S5732-H-V2.

Attribute

Alarm ID	OID	Alarm Severity	Alarm Type
67699723	1.3.6.1.4.1.2011.5.25.667.2.19	Major	Processing error alarm

Parameters

Parameter	Description
RemoteUnitEsn	ESN of the RU.
InterfaceName	Interconnection port.
Firmware	Firmware type. The value can be APP, PoE, or BIOS.

Parameter	Description
Reason	Failure cause. - no ack received: The RU does not send a response during the upgrade. - upgrade is break: The upgrade is interrupted. The typical scenario is that the RU is reset during the upgrade. - no signature: The new firmware used for upgrade does not have a signature.

Impact on the System

This alarm is generated when the central switch fails to upgrade an RU. This alarm needs to be manually cleared.

Possible Causes

- Cause 1: The RU does not send a response during the upgrade.
- Cause 2: The upgrade is interrupted. The typical scenario is that the RU is reset during the upgrade.
- Cause 3: The new firmware used for upgrade does not have a signature.

Procedure

- Cause 1: The RU does not send a response during the upgrade.
If the Reason field in the alarm information is "no ack received", check whether the communication between the central switch and the RU is normal.
- Cause 2: The upgrade is interrupted. The typical scenario is that the RU is reset during the upgrade.
If the Reason field in the alarm information is "upgrade is break", no action is required. The RU will be upgraded again.
- Cause 3: The new firmware used for upgrade does not have a signature.
If the Reason field in the alarm information is "no signature", the signature of the firmware patch is incorrect. In this case, contact the firmware patch provider to check whether the signature in the patch is correct.

3.5.3.38 ALM-67699726 hwRuMngOffline

Description

The remote-unit is offline. (RemoteUnitEsn=[RemoteUnitEsn], ConnectInterface=[ConnectInterface], Reason=[Reason])

The RU goes offline.

NOTE

This alarm is supported only on S5735I-L-V2, S6730-H-V2, S5732-H-V2.

Attribute

Alarm ID	OID	Alarm Severity	Alarm Type
67699726	1.3.6.1.4.1.2011.5 .25.667.2.25	Major	Processing error alarm

Parameters

Parameter	Description
RemoteUnitEsn	ESN of the RU.
ConnectInterface	Interconnection port.
Reason	Disconnection reason.

Impact on the System

The RU goes offline.

Possible Causes

- Unknown: The RU goes offline due to unknown reasons.
- No heartbeat: The RU goes offline since no heartbeat is detected.
- Port down: The RU goes offline because the port is Down.
- Multi-RU on port: A port is connected to multiple RUs.
- Manual: The RU goes offline after it is manually restarted.
- Upgrade: The RU goes offline after it is upgraded and restarted.

Procedure

- Unknown: The RU goes offline due to unknown reasons.
Collect alarm and configuration information, and contact technical support personnel.
- No heartbeat: The RU goes offline since no heartbeat is detected.
Check whether the RU's link or the RU is faulty, and contact technical support personnel.
- Port down: The RU goes offline because the port is Down.
Check why the port is Down
- Multi-RU on port: A port is connected to multiple RUs.

Check whether a port is connected to multiple RUs. An Eth-Trunk interface can connect to only one online RU.

- Manual: The RU goes offline after it is manually restarted.
This is a normal situation, and no action is required.
- Upgrade: The RU goes offline after it is upgraded and restarted.
This is a normal situation, and no action is required.

3.5.3.39 ALM-67699725 hwRuMngOnline

Description

The remote-unit is online. (RemoteUnitEsn=[RemoteUnitEsn], ConnectInterface=[ConnectInterface])

The RU goes online.

NOTE

This alarm is supported only on S5735I-L-V2, S6730-H-V2, S5732-H-V2.

Attribute

Alarm ID	OID	Alarm Severity	Alarm Type
67699725	1.3.6.1.4.1.2011.5.25.667.2.23	Major	Processing error alarm

Parameters

Parameter	Description
RemoteUnitEsn	ESN of the RU.
ConnectInterface	Interconnection port.

Impact on the System

The RU goes online normally.

Possible Causes

The RU goes online normally.

Procedure

This log is informational only and no action is required.

3.5.3.40 ALM-67706884 hwRuPortCrcErrorRising

Description

Remote unit CRC error is rising. (RemoteUnitEsn=[RemoteUnitEsn], InterfaceName=[InterfaceName], CrcErrorStatistics=[CrcErrorStatistics], CrcErrorThreshold=[CrcErrorThreshold], CrcErrorInterval=[CrcErrorInterval](s))

The number of interface CRC errors on the remote module exceeded the threshold.

NOTE

This alarm is supported only on S5735-L-V2, S5735-S-V2, S5735I-S-V2, S5735I-L-V2, S6730-H-V2, S5732-H-V2.

Attribute

Alarm ID	OID	Alarm Severity	Alarm Type
67706884	1.3.6.1.4.1.2011.5.25.667.2.9	Major	Quality of service alarm

Parameters

Parameter	Description
RemoteUnitEsn	ESN of the remote module.
InterfaceName	Port number of the remote module.
CrcErrorStatistics	Statistics in a CRC period.
CrcErrorThreshold	CRC alarm threshold. The value is fixed at 20.
CrcErrorInterval	Alarm period. The value is fixed at 60s.

Impact on the System

Some service data on the port is discarded.

Possible Causes

- Cause 1: transceiver fault.
- Cause 2: Fiber failure.

Procedure

- Cause 1: transceiver fault.
Replace the optical module and check whether the alarm is cleared.

- If so, no further action is required.
 - If not, collect alarm and configuration information, and contact technical support.
- Cause 2: Fiber failure.
Replace the optical fiber and check whether the alarm is cleared.
 - If so, no further action is required.
 - If not, collect alarm and configuration information, and contact technical support.

3.5.4 Firewall Alarms

3.5.4.1 ALM-15795462 hwGtlDataDamaged

Description

The license fails to be activated during system startup because the license data is damaged. (Position=[hwGtlPosition])

The license fails to be activated during system startup because the current license data is damaged.

Attribute

Alarm ID	OID	Alarm Severity	Alarm Type
15795462	1.3.6.1.4.1.2011.5 .25.142.2.56	Critical	Quality of service alarm

Parameters

Parameter	Description
hwGtlPosition	Location of the license data.

Impact on the System

Related service functions may be unavailable or configurations may become invalid.

Possible Causes

The license data on the device is damaged. As a result, the license fails to be activated during system startup.

Procedure

Reactivate a license file.

3.5.4.2 ALM-15795028 hwlIPSecNegoFail

Description

IPSec tunnel negotiation fails. (Ifindex=[Ifindex], SeqNum=[SeqNum], Reason=[Reason-Str], ReasonCode=[ReasonCode], PeerAddress=[PeerAddress], PeerPort=[PeerPort], VsysName=[vsys-name], InterfaceName=[InterfaceName])

Attribute

Alarm ID	OID	Alarm Severity	Alarm Type
15795028	1.3.6.1.4.1.2011.6 .122.26.6.14	Warning	Quality of service alarm

Parameters

Parameter	Description
Ifindex	Indicates the index of the interface on the IPsec tunnel.
SeqNum	Indicates the sequence number of the IPsec policy.
Reason-Str	Indicates the reason of IPsec tunnel negotiation failure.
ReasonCode	Indicates the reason code of IPsec tunnel negotiation failure.
PeerAddress	Indicates the remote IP address.
PeerPort	Indicates the remote UDP port number.
vsys-name	Name of the virtual system to which an IPsec policy belongs. The value is fixed to Public.
InterfaceName	Indicates the interface name.

Impact on the System

An IPsec tunnel fails to be established.

Possible Causes

The possible causes are as follows:

- phase1 proposal mismatch: IKE proposal parameters on both ends do not match. This field is displayed only on the tunnel initiator.
- phase1 proposal encryption algorithm mismatch: Encryption algorithm parameters in IKE proposals on both ends do not match. This field is displayed only on the tunnel responder.
- phase1 proposal authentication method mismatch: Authentication method parameters in IKE proposals on both ends do not match. This field is displayed only on the tunnel responder.
- phase1 proposal authentication algorithm mismatch: Authentication algorithm parameters in IKE proposals on both ends do not match. This field is displayed only on the tunnel responder.
- phase1 proposal dh mismatch: DH group parameters in IKE proposals on both ends do not match. This field is displayed only on the tunnel responder.
- phase1 proposal integrity algorithm mismatch: Integrity algorithm parameters in IKE proposals on both ends do not match. This field is displayed only on the tunnel responder.
- phase1 proposal prf mismatch: PRF algorithm parameters in IKE proposals on both ends do not match. This field is displayed only on the tunnel responder.
- phase2 proposal or pfs mismatch: IPsec proposal parameters, pfs algorithm, or security ACL of the two ends do not match.
- responder dh mismatch: The DH algorithm of the responder does not match.
- initiator dh mismatch: The DH algorithm of the initiator does not match.
- encapsulation mode mismatch: The encapsulation mode does not match.
- flow or peer mismatch: The security ACL or IKE peer address of the two ends does not match.
- version mismatch: The IKE version number of the two ends does not match.
- peer address mismatch: The IKE peer address of the two ends does not match.
- config ID mismatch: The IKE peer of the specified ID is not found.
- exchange mode mismatch: The negotiation mode of the two ends does not match.
- authentication fail: Identity authentication fails.
- construct local ID fail: The local ID fails to be constructed.
- rekey no find old sa: The old SA is not found during re-negotiation.
- rekey fail: The old SA is going offline during re-negotiation.
- first packet limited: The rate of the first packet is limited.
- unsupported version: The IKE version number is not supported.
- malformed message: Malformed message.
- malformed payload: Malformed payload.
- malformed payload or psk mismatch: Malformed payload or pre-share-key mismatch.
- critical drop: Unidentified critical payload.
- cookie mismatch: Cookie mismatch.
- invalid cookie: Invalid cookie.
- invalid length: Invalid packet length.

- unknown exchange type: Unknown negotiation mode.
- uncritical drop: Unidentified non-critical payload.
- route limit: The number of injected routes has reached the upper limit.
- ip assigned fail: IP address allocation fails.
- eap authentication timeout: EAP authentication times out.
- eap authentication fail: EAP authentication fails.
- xauth authentication fail: XAUTH authentication fails.
- xauth authentication timeout: XAUTH authentication timeout.
- license or specification limited: License limit.
- local address mismatch: The local IP address in IKE negotiation and interface IP address do not match.
- dynamic peers number reaches limitation: The number of IKE peers reaches the upper limit.
- ipsec tunnel number reaches limitation: The number of IPsec tunnels reaches the upper limit.
- netmask mismatch: The mask does not match the configured mask after the IPsec mask filtering function is enabled.
- flow conflict: A data flow conflict occurs.
- proposal mismatch or use sm in ikev2: IPsec proposals at both ends of the IPsec tunnel do not match or IKEv2 uses the SM algorithm.
- ikev2 not support sm in ipsec proposal ikev2: IKEv2 does not support the SM algorithm used in the IPsec proposal.
- no policy applied on interface: No policy is applied to an interface.
- nat detection fail: NAT detection failed.
- fragment packet limit: Fragment packets exceed the limit.
- fragment packet reassemble timeout: Fragment packet reassembly times out.

Procedure

- Cause: phase1 proposal mismatch

Check IKE proposal parameters at both ends of the IPsec tunnel and ensure that the parameters are consistent at both ends.

- Cause: phase2 proposal or pfs mismatch

Check IPsec proposal parameters or PFS algorithms at both ends of the IPsec tunnel and ensure that the parameters or algorithms are consistent at both ends.

- Cause: responder dh mismatch, initiator dh mismatch

Check DH algorithms at both ends of the IPsec tunnel and ensure that the algorithms are consistent at both ends.

- Cause: encapsulation mode mismatch

Check encapsulation modes at both ends of the IPsec tunnel and ensure that the encapsulation modes are consistent at both ends.

- Cause: eap authentication timeout, eap authentication fail, xauth authentication fail, xauth authentication timeout

Ensure that the client's user name and password as well as user access configuration are correct.

- Cause: ip assigned fail

Ensure that the AAA and IPsec configurations, such as the IP pool, AAA service scheme, and IP addresses assigned to IKE users, are correct.

- Cause: peer address mismatch

Check the IP addresses of IKE peers at both ends and ensure that the IP addresses match each other.

- Cause: config ID mismatch

Check identity authentication parameters, such as the ID type and ID value, and ensure that the parameters match each other.

- Cause: authentication fail

Check IKE proposal parameters or IKE peer parameters at both ends of the IPsec tunnel and ensure that the parameters are consistent at both ends.

- Cause: license or specification limited

Apply for a license or expand the capacity as required.

- Cause: exchange mode mismatch

Check the IKEv1 phase 1 negotiation modes at both ends and ensure that the negotiation modes are consistent at both ends.

- Cause: route limit

Replace the device with the one that has a higher route specification and plan the network properly.

- Cause: local address mismatch

Check the local IP address and interface IP address used in IKE negotiation and ensure that the IP addresses are consistent.

- Cause: ipsec tunnel number reaches limitation

Delete unnecessary IPsec tunnels or expand the capacity.

- Cause: dynamic peers number reaches limitation

Expand the capacity and plan the network properly.

- Cause: in disconnect state

Check whether the link or device is working properly based on the IPsec link detection result.

- Cause: proposal mismatch or use sm in ikev2, ikev2 not support sm in ipsec proposal

Check the algorithm used by IKEv2 in the IPsec proposal and ensure that the algorithm is correct.

- Cause: flow conflict

Check ACL rules at both ends of the IPsec tunnel and ensure that the ACLs are correct.

- Cause: netmask mismatch

Change the IPsec-protected data flow range of the branch or headquarters to ensure that the data flow ranges negotiated by the branch and headquarters do not overlap.

- Cause: no policy applied on interface

Apply the required IPsec policy to the interface.

- Cause: fragment packet limit

The number of received fragmented packets exceeds the limit. Adjust the MTU of the peer device correctly.

- Cause: fragment packet reassemble timeout

Ensure that the links at both ends are normal and the device status is normal.

- If the fault persists, collect related information and contact technical support personnel.

3.5.5 S380 Device Alarms

3.5.5.1 ALM-135463092 hwChassisFail

Description

The chassis partially failed. (EntPhysicalIndex=[EntPhysicalIndex], EntPhysicalName=[EntPhysicalName], EntityTrapFaultID=[EntityTrapFaultID], Reason=[Reason])

A chassis experienced a partial failure.

Attribute

AlarmID	Alarm OID	Alarm Severity	Alarm Type
135463092	1.3.6.1.4.1.2011.5.25 .219.2.1.3	Critical	Equipment alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
EntPhysicalIndex	Index of a physical entity.
EntPhysicalName	Entity name.

Name	Meaning
EntityTrapFaultID	Alarm cause.
Reason	

Impact on the System

The system may become abnormal.

Possible Causes

- Cause 1: Different SFUs were installed in the same chassis.
- Cause 2: The system power or the power of the backup power supply is insufficient.
- Cause 3: No SFU is present in the chassis.
- Cause 4: No LPU is present in the chassis.
- Cause 5: No CMU is present in the chassis.
- Cause 6: The power module types are inconsistent.
- Cause 7: Failed to obtain slot information of the power supply.
- Cause 8: There is two or more fans not detected.
- Cause 9: The number of detected SFUs does not meet requirements.

Procedure

- Cause 1: Different SFUs were installed in the same chassis.
 1. Insert the correct SFU.
- Cause 2: The system power or the power of the backup power supply is insufficient.
 1. Add a power module.
- Cause 3: No SFU is present in the chassis.
 1. Insert the SFU.
- Cause 4: No LPU is present in the chassis.
 1. Insert the LPU.
- Cause 5: No CMU is present in the chassis.
 1. Insert the CMU.
- Cause 6: The power module types are inconsistent.
 1. Install only DC or AC power modules into all the power slots on the device.
- Cause 7: Failed to obtain slot information of the power supply.
 1. Insert the power module into another slot. If the alarm persists, replace the power module.
- Cause 8: There is two or more fans not detected.
 1. Install all the fan modules.
- Cause 9: The number of detected SFUs does not meet requirements.

1. Insert the SFU.

3.5.5.2 ALM-134292070 hwPoePowerOff

Description

PD powered off. (IfIndex=[IfIndex], Interface=[Interface], FaultID=[FaultID])

PD powered off.

 NOTE

Only the S380-L and S380-S series support this alarm.

Attribute

AlarmID	Alarm OID	Alarm Severity	Alarm Type
134292070	1.3.6.1.4.1.2011.5.25 .195.40.2	Warning	Equipment alarm

Parameters

Name	Meaning
IfIndex	Indicates the index of the faulty interface.
Interface	Indicates the faulty interface name.
FaultID	Error code.

Impact on the System

The PD connected to the interface is powered off and cannot work normally.

Possible Causes

1. The PD is removed.
2. The PD is faulty.
3. When the power is insufficient, the interface with a higher priority preempts the power.
4. The interface to which the PD connects is automatically powered off in the power-off time range.
5. The PD is powered off because of overcurrent protection.

Procedure

1. Check whether the PD is removed.
If so, go to step 2.
If not, go to step 4.
2. Check whether the PD is removed because of a normal operation.
If so, the alarm handling ends.
If not, go to step 3.
3. Install the PD to check whether it is powered on.
If so, the alarm handling ends.
If not, go to step 4.
4. Run the **display poe power-state** *interface-type interface-number* command to check whether the maximum output power of the interface is sufficient.
If so, go to step 5.
If not, connect the PD to another interface or PoE device.
5. Run the **display poe power-state** *interface-type interface-number* command to check whether the power supply priority of the interface is low.
If so, go to step 6.
If not, go to step 8.
6. Check whether the power supply priority of the interface needs to be reconfigured.
If so, go to step 6.
If not, go to step 7.
7. Run the **poe priority** command to configure the power supply priority of the interface. Then check whether the PD is powered on.
If so, the alarm handling ends.
If not, go to step 8.
8. Run the **display poe power-state** *interface-type interface-number* command to check whether the interface is in the power-off time range.
If so, the alarm handling ends.
If not, go to step 9.
9. Check whether the PD is faulty.
If so, replace it.
If not, collect alarm information and configuration information, and then contact technical support personnel.

3.5.5.3 ALM-15795219 hwPoePowerOverUtilizationThreshold

Description

POE/4/PWRUTITHRESH: OID [oid] PSE power consumption has exceeded the upper limit. (ChassisID=[INTEGER], ConsumingPower=[INTEGER], PowerThreshold=[INTEGER])

PSE power consumption has exceeded the upper limit.

 NOTE

Only the S380-L and S380-S series support this alarm.

Attribute

AlarmID	Alarm OID	Alarm Severity	Alarm Type
15795219	1.3.6.1.4.1.2011.5.25 .195.40.17	Warning	Equipment alarm

Parameters

Name	Meaning
DeviceID	Indicates the device ID.
ConsumingPower	Indicates the current power consumption.
PowerThreshold	Indicates the power threshold.

Impact on the System

If the alarm persists, all the PDs may be powered off because of insufficient power supply.

Possible Causes

The total power consumption of all the PDs is greater than or equal to the alarm threshold.

Procedure

1. Check whether the power consumption of the PDs is within the accepted range.
 - If so, go to step 2.
 - If not, go to step 3.
2. Run the **poe-power utilization-threshold** command to change the alarm threshold for PoE power consumption percentage.
3. Replan the network based on the system external power supply capability. Run the **poe priority** command to increase the priority of important PDs to prevent their power from being occupied by other PDs. Power off the PDs that are not required to ensure system reliability.

3.5.5.4 ALM-135463086 hwIfMonitorInputRateRising

Description

Interface input flow bandwidth usage exceeded the trap threshold.
(Interface=[IfIndex], BandWidthUsage=[hwIfMonitorInputRatePercentage],
TrapThreshold=[hwIfMonitorInputRateThreshold],
InterfaceName=[InterfaceName])

This object indicates that an alarm is generated when the percentage of the traffic received by an interface to the total bandwidth of the interface exceeds the threshold.

Attribute

AlarmID	Alarm OID	Alarm Severity	Alarm Type
135463086	1.3.6.1.4.1.2011.5.25 .41.4.5	Warning	Processing error alarm

Parameters

Parameter	Description
IfIndex	Interface index
hwIfMonitorInputRatePercentage	Input traffic statistics.
hwIfMonitorInputRateThreshold	Input traffic alarm threshold.
InterfaceName	Interface name.

Impact on the System

When the traffic is close to 100% of the bandwidth, delay or packet loss may occur.

Possible Causes

The rate of traffic received by the interface was too large.

Procedure

1. Run the **display this interface** command in the interface view to check whether the traffic threshold is too low. Determine the alarm threshold based on service requirements.

- If yes, go to Step 2.
- If not, go to Step 3.

2. Run the **trap-threshold input-rate *bandwidth-in-use*** command in the interface view to reconfigure the alarm threshold. Then check whether the alarm is cleared.
 - If yes, go to Step 4.
 - If not, go to Step 3.
3. Collect alarm and configuration information, and contact technical support personnel.
4. End.

3.5.5.5 ALM-135463087 hwIfMonitorOutputRateRising

Description

Interface output flow bandwidth usage exceeded the trap threshold.
(Interface=[IfIndex], BandWidthUsage=[hwIfMonitorOutputRatePercentage],
TrapThreshold=[hwIfMonitorOutputRateThreshold],
InterfaceName=[InterfaceName])

This object indicates that an alarm is generated when the ratio of the traffic sent by an interface to the total bandwidth of the interface exceeds the threshold.

Attribute

AlarmID	Alarm OID	Alarm Severity	Alarm Type
135463087	1.3.6.1.4.1.2011.5.25 .41.4.7	Warning	Processing error alarm

Parameters

Parameter	Description
IfIndex	Interface index
hwIfMonitorOutputRatePercentage	Output traffic statistics.
hwIfMonitorOutputRateThreshold	Output traffic alarm threshold.
InterfaceName	Interface name.

Impact on the System

When the traffic is close to 100% of the bandwidth, delay or packet loss may occur.

Possible Causes

The rate of traffic sent by the interface was too large.

Procedure

1. Run the **display this interface** command in the interface view to check whether the traffic threshold is too low. Determine the alarm threshold based on service requirements.
 - If yes, go to step 2.
 - If not, go to Step 3.
2. Run the **trap-threshold output-rate *bandwidth-in-use*** command in the interface view to reconfigure the alarm threshold. Then check whether the alarm is cleared.
 - If yes, go to Step 4.
 - If not, go to Step 3.
3. Collect alarm and configuration information, and contact technical support personnel.
4. End.

3.5.5.6 ALM-230432775 hwUsedIPReachThreshold

Description

The number of used addresses exceeds alarm threshold. (PoolName=[poolname], Threshold=[threshold])

The number of used addresses exceeds alarm threshold.

Attribute

AlarmID	Alarm OID	Alarm Severity	Alarm Type
230432775	1.3.6.1.4.1.2011.6.8.2.2.0.6	Warning	Quality of service alarm

Parameters

Parameter	Description
poolname	Address pool name.
threshold	Percentage of the alarm indicating that the addresses in an address pool are used up.

Impact on the System

IP addresses may fail to be allocated.

Possible Causes

The number of access users increased and the usage of the address pool exceeded the threshold.

Procedure

- Add more allocatable IP addresses to the address pool by reducing the mask length. Run the `ip address ip-address { mask | mask-length }` command in the interface view to reduce the mask length. Alternatively, run the `network ip-address [ mask { mask | mask-length } ]` command in the global address pool view to reduce the mask length.
- If an IP address segment is configured in the address pool, add more allocatable IP addresses to the address pool by increasing the range of the IP address segment. Run the `dhcp server ip-range start-ip-address end-ip-address` command in the interface view to increase the range of IP addresses. Alternatively, run the `section section-id start-address [ end-address ]` command in the global address pool view to increase the range of IP addresses.

3.5.5.7 ALM-157163553 hwMacUsageRaisingInfo

Description

MAC usage reached the Threshold. (PhysicalName=[entPhysicalName], MacEntityUsage=[hwMacEntityUsage], MacEntityUsageThreshold=[hwMacEntityUsageThreshold].)

The MAC address table usage exceeded the threshold.

Attribute

AlarmID	Alarm OID	Alarm Severity	Alarm Type
157163553	1.3.6.1.4.1.2011.5.25.42.2.1.7.1	Warning	Quality of service alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
entPhysicalName	NE Name
hwMacEntityUsage	MAC table usage
hwMacEntityUsageThreshold	Alarm threshold for MAC address table usage

Impact on the System

After the MAC address usage reaches the alarm threshold, some MAC addresses may fail to be learned.

Possible Causes

The MAC address table usage reaches 80% of the threshold.

Procedure

- Delete unnecessary static MAC address entries. See **mac-address static vlan**.

3.5.5.8 ALM-157155346 hwmflpVlanLoopAlarm

Description

MAC flapping detected, VlanId = [VlanId], Original-Port = [IfNameA], Flapping port 1 = [IfNameB], port 2 = [IfNameC]. [AlarmReason].

MAC address flapping occurs in a VLAN.

Attribute

AlarmID	Alarm OID	Alarm Severity	Alarm Type
157155346	1.3.6.1.4.1.2011.5.25 .160.3.13	Warning	Quality of service alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
VlanId	VLAN ID.
IfNameA	Drift source port.
IfNameB	Destination port of the floating IP address.
IfNameC	Destination port of the floating IP address.
AlarmReason	Alarm cause.

Impact on the System

Traffic cannot be forwarded.

Possible Causes

There may be loops on the current network.

Procedure

Configure the error-down function on the interface or eliminate loops on the network.

3.5.5.9 ALM-15795035 hwSecStatSessOverThreshold

Description

Total number of sessions on slot[hwSecStatSessTrapSlot] CPU[hwSecStatSessTrapCPU] is [hwSecStatSessTrapCount], exceeding threshold value [hwSecStatSessTrapThreshold].

The number of IPv4 sessions on a single CPU exceeded the alarm threshold.

Attribute

AlarmID	Alarm OID	Alarm Severity	Alarm Type
15795035	1.3.6.1.4.1.2011.6.12 2.15.3.2.1	Minor	Quality of service alarm

Parameters

Name	Meaning
hwSecStatSessTrapSlot	Slot No.
hwSecStatSessTrapCPU	CPU ID
hwSecStatSessTrapCount	Total number of sessions
hwSecStatSessTrapThreshold	Session alarm threshold

Impact on the System

If the number of IPv4 sessions on a single CPU exceeds the upper limit, new sessions cannot be created and packet loss occurs.

Possible Causes

The total number of IPv4 sessions of a CPU exceed the alarm threshold.

Procedure

Check whether the session node recycling and aging are correct.

3.5.5.10 ALM-15795035 hwPacketDiscard

Description

Packets are forwarded properly.
(DiscardReason=[DiscardReason],InterfaceName=[InterfaceName])

Packets to be forwarded are discarded.

Attribute

AlarmID	Alarm OID	Alarm Severity	Alarm Type
15795582	1.3.6.1.4.1.2011.6.12 2.15.3.2.1	Minor	Quality of service alarm

Parameters

Name	Meaning
DiscardReason	Discard Reason
InterfaceName	Interface name

Impact on the System

Packets cannot be forwarded.

Possible Causes

The addresses in the NAT address pool are insufficient.

Procedure

Check the NAT configuration and check whether the address resources in the address pool are sufficient. If the address resources are insufficient, modify the range of addresses in the address pool.

3.5.5.11 ALM-139591683 linkDown

Description

The interface status changes. (ifName=[ifName], AdminStatus=[ifAdminStatus], OperStatus=[ifOperStatus], Reason=[Reason], mainIfname=[mainIf])

The interface status changes.

Attribute

Alarm ID	OID	Alarm Severity	Alarm Type
139591683	1.3.6.1.6.3.1.1.5.3	Major	Equipment alarm

Parameters

Name	Meaning
ifName	Interface name
ifAdminStatus	Interface admin status.
ifOperStatus	Current interface status
Reason	Reason for trap generation
mainIf	Name of the main interface

Impact on the System

The interface cannot forward packets normally.

Possible Causes

- Cause 1: Interface physical link is down.
- Cause 2: LACP negotiation failed.
- Cause 3: Receive ConfReq packet.
- Cause 4: Receive ConfAck packet.
- Cause 5: Receive Nak packet.
- Cause 6: Receive Term packet.
- Cause 7: Receive TermAck packet.
- Cause 8: Receive CodeRej packet.
- Cause 9: Receive ProtoRej packet.
- Cause 10: CHAP authentication failed.
- Cause 11: PAP authentication failed.
- Cause 12: Keepalive timer expires.
- Cause 13: The PVC is Down.
- Cause 14: EFM DOWN.
- Cause 15: The tunnel is down.
- Cause 16: The interface is shut down.
- Cause 17: The link protocol is down.

- Cause 19: The link protocol is up.
- Cause 20: The main interface is down.
- Cause 21: Interface physical link is up.
- Cause 22: The conditions for the activation of the interface are not met.
- Cause 23: The conditions for the activation of the interface are met
- Cause 24: The tunnel is up.
- Cause 25: The interface is deleted.
- Cause 26: BFD session is down.
- Cause 27: BFD session is up.
- Cause 28: EFM UP
- Cause 30: DLDP detect down.
- Cause 31: DLDP detect up.
- Cause 32: VRRP FLOW DOWN.
- Cause 33: VRRP FLOW UP.
- Cause 34: VE FLOW DOWN.
- Cause 35: VE FLOW UP.
- Cause 36: The interface is error down.
- Cause 37: CRC ERR DOWN.
- Cause 38: CRC ERR UP
- Cause 39: Transceiver speed does not match the speed configured on the port.
- Cause 40: The port does not support current transceiver.
- Cause 41: Transceiver does not support the negotiation configuration on the port.
- Cause 43: The interface is trigger down.
- Cause 48: CFM DOWN.
- Cause 49: CFM UP.
- Cause 51: The sub-interface linkDown alarm is disabled.

Procedure

- Cause 1: Interface physical link is down.
 - a. Run the **display this** command in the interface view to check whether the interfaces at both ends are shut down. If the interfaces are sub-interfaces, check whether VLAN IDs are configured for the interfaces at both ends.
 - If the interface is a sub-interface, run the **vlan-type dot1q** command to configure a correct VLAN ID for the sub-interface. Then, check whether the alarm is cleared. If the alarm persists, go to Step 2.
 - If the interface is not shut down, go to Step 2.
 - b. Check whether the physical link is normal, for example, whether the network cable or optical module is loose or disconnected.
 - If the physical link is abnormal, reconnect the physical link and check whether the alarm is cleared. If the alarm persists, go to Step 3.

- If the physical link works properly, go to Step 3.
- c. Collect alarm and configuration information, and contact technical support personnel.
- Cause 2: LACP negotiation failed.
 - a. Run the **display interface** command in the system view to check whether the local or remote interface is Down.
 - If either interface is Down, run the **undo shutdown** command in the interface view, and then check whether the alarm is cleared. If the alarm is not cleared, go to Step 2.
 - If the interface status is Up, go to Step 2.
 - b. Run the **display interface eth-trunk** command in the system view to check whether the number of local and remote interfaces that are added to an Eth-Trunk is greater than the upper threshold for the number of member links.
 - If the number of local and remote interfaces that are added to the Eth-Trunk is greater than the upper threshold for the number of member links, run the **max active-linknumber** command in the Eth-Trunk interface view to configure a proper upper threshold for the number of member links, and then check whether the alarm is cleared. If the alarm is not cleared, go to Step 4.
 - If the number of local and remote interfaces that are added to the Eth-Trunk is smaller than the upper threshold for the number of member links, go to Step 3.
 - c. Run the **display interface eth-trunk** command in the system view to check whether the number of local and remote interfaces that are added to an Eth-Trunk is smaller than the lower threshold for the number of member links.
 - If the number of local and remote interfaces that are added to the Eth-Trunk is smaller than the lower threshold for the number of member links, run the **least active-linknumber** command in the Eth-Trunk interface view to configure a proper lower threshold for the number of member links, and then check whether the alarm is cleared. If the alarm is not cleared, go to Step 4.
 - If the number of local and remote interfaces that are added to the Eth-Trunk is smaller than the lower threshold for the number of member links is greater than the lower threshold of member links on the Eth-Trunk interface, go to Step 4.
 - d. Collect alarm information and configuration information, and then contact technical support personnel.
- Cause 3: Receive ConfReq packet.
 - a. Run the **display interface** command in the system view to check whether the PPP protocol of the remote device is works properly.
 - If the PPP protocol of the remote device works properly, run the **display interface** command to check the physical link statuses of the devices (including the intermediate device), such as the number of

lost packets and error packets. If the physical link statuses are normal but the alarm is not cleared, go to Step 2.

- If the PPP protocol of the remote device works improperly, contact the engineer responsible for the remote device to rectify the fault. If the fault is rectified but the alarm is not cleared, go to Step 2.
- b. Collect alarm information and configuration information, and then contact technical support personnel.
- Cause 4: Receive ConfAck packet.
 - a. Run the **display interface** command in the system view to check whether the PPP protocol of the remote device is works properly.
 - If the PPP protocol of the remote device works properly, run the **display interface** command to check the physical link statuses of the devices (including the intermediate device), such as the number of lost packets and error packets. If the physical link statuses are normal but the alarm is not cleared, go to Step 2.
 - If the PPP protocol of the remote device works improperly, contact the engineer responsible for the remote device to rectify the fault. If the fault is rectified but the alarm is not cleared, go to Step 2.
 - 2. Collect alarm information and configuration information, and then contact technical support personnel.
- Cause 5: Receive Nak packet.
 - a. Run the **display interface** command in the system view to check whether the PPP protocol of the remote device is works properly.
 - If the PPP protocol of the remote device works properly, run the **display interface** command to check the physical link statuses of the devices (including the intermediate device), such as the number of lost packets and error packets. If the physical link statuses are normal but the alarm is not cleared, go to Step 2.
 - If the PPP protocol of the remote device works improperly, contact the engineer responsible for the remote device to rectify the fault. If the fault is rectified but the alarm is not cleared, go to Step 2.
 - b. Collect alarm information and configuration information, and then contact technical support personnel.
- Cause 6: Receive Term packet.
 - a. Run the **display interface** command in the system view to check whether the PPP protocol of the remote device is works properly.
 - If the PPP protocol of the remote device works properly, run the **display interface** command to check the physical link statuses of the devices (including the intermediate device), such as the number of lost packets and error packets. If the physical link statuses are normal but the alarm is not cleared, go to Step 2.
 - If the PPP protocol of the remote device works improperly, contact the engineer responsible for the remote device to rectify the fault. If the fault is rectified but the alarm is not cleared, go to Step 2.
 - b. Collect alarm information and configuration information, and then contact technical support personnel.

- Cause 7: Receive TermAck packet.
 - a. Run the **display interface** command in the system view to check whether the PPP protocol of the remote device is works properly.
 - If the PPP protocol of the remote device works properly, run the display interface command to check the physical link statuses of the devices (including the intermediate device), such as the number of lost packets and error packets. If the physical link statuses are normal but the alarm is not cleared, go to Step 2.
 - If the PPP protocol of the remote device works improperly, contact the engineer responsible for the remote device to rectify the fault. If the fault is rectified but the alarm is not cleared, go to Step 2.
 - b. Collect alarm information and configuration information, and then contact technical support personnel.
- Cause 8: Receive CodeRej packet.
 - a. Run the **display interface** command in the system view to check whether the PPP protocol of the remote device is works properly.
 - If the PPP protocol of the remote device works properly, run the **display interface** command to check the physical link statuses of the devices (including the intermediate device), such as the number of lost packets and error packets. If the physical link statuses are normal but the alarm is not cleared, go to Step 2.
 - If the PPP protocol of the remote device works improperly, contact the engineer responsible for the remote device to rectify the fault. If the fault is rectified but the alarm is not cleared, go to Step 2.
 - b. Collect alarm information and configuration information, and then contact technical support personnel.
- Cause 9: Receive ProtoRej packet.
 - a. Run the **display interface** command in the system view to check whether the PPP protocol of the remote device is works properly.
 - If the PPP protocol of the remote device works properly, run the **display interface** command to check the physical link statuses of the devices (including the intermediate device), such as the number of lost packets and error packets. If the physical link statuses are normal but the alarm is not cleared, go to Step 2.
 - If the PPP protocol of the remote device works improperly, contact the engineer responsible for the remote device to rectify the fault. If the fault is rectified but the alarm is not cleared, go to Step 2.
 - b. Collect alarm information and configuration information, and then contact technical support personnel.
- Cause 10: CHAP authentication failed.
 - a. Run the **display this** command in the interface view to check whether the local end is a server end (authenticating end) or a client end (authenticated end).
 - If the local end is the server end, check whether the user and password configured on the remote end are correct. If they are

incorrect, run the local-user password command in the AAA view to re-configure them. Then, check whether the alarm is cleared. If the alarm is not cleared, go to Step 2.

- If the local end is the client end, run the **display this** command to check whether the user and password configured on the local end are correct. If they are incorrect, run the local-user password command in the AAA view to re-configure them. Then, check whether the alarm is cleared. If the alarm is not cleared, go to Step 2.
- b. Collect alarm information and configuration information, and then contact technical support personnel.
- Cause 11: PAP authentication failed.
 - a. Run the **display this** command in the interface view to check whether the local end is a server end (authenticating end) or a client end (authenticated end).
 - If the local end is the server end, check whether the user and password configured on the remote end are correct. If they are incorrect, run the **local-user password** command in the AAA view to re-configure them. Then, check whether the alarm is cleared. If the alarm is not cleared, go to Step 2.
 - If the local end is the client end, run the **display this** command to check whether the user and password configured on the local end are correct. If they are incorrect, run the local-user password command in the AAA view to re-configure them. Then, check whether the alarm is cleared. If the alarm is not cleared, go to Step 2.
 - 2. Collect alarm information and configuration information, and then contact technical support personnel.
- Cause 12: Keepalive timer expires.
 - a. Run the **display interface** command in the system view to check whether the PPP protocol of the remote device works properly.
 - If the PPP protocol of the remote device works properly, run the **display interface** command to check the physical link statuses of the devices (including the intermediate device), such as the number of lost packets and error packets. If the physical link statuses are normal but the alarm is not cleared, go to Step 2.
 - If the PPP protocol of the remote device works improperly, contact the engineer responsible for the remote device to rectify the fault. If the fault is rectified but the alarm is not cleared, go to Step 2.
 - b. Collect alarm information and configuration information, and then contact technical support personnel.
- Cause 13: The PVC is Down.
 - a. Run the **display this** command in the sub-interface view to check whether the interfaces on both ends are shut down.
 - If the interfaces are shut down, go to Step 4.

- If the interfaces are not shut down, go to Step 2.
 - b. Run the **display fr interface** command in the system view to check the physical and protocol status of the main interface.
 - If the physical status of the main interface is Down, go to Step 5.
 - If the physical status of the main interface is Up but the protocol status is Down, go to Step 6.
 - If the both the physical and protocol status of the main interface is Up, go to Step 3.
 - c. Ask engineers of the peer end to check whether the PVC status is Active.
 - If the PVC status on the peer end is Active, go to Step 7.
 - If the PVC status on the peer end is Inactive, go to Step 8.
 - d. Run the **undo shutdown** command to start the sub-interface.
 - e. Check the physical connection of the main interface.
 - f. Check the LMI configurations.
 - g. Collect alarm information and configuration information, and then contact technical support personnel.
 - h. End.
- Cause 14: EFM DOWN.
 - a. Run the **display efm session** command in the system view to check whether the EFM state field is displayed as Detect.
 - If the EFM state field is displayed as Detect, go to Step 3.
 - If the EFM state field is not displayed as Detect, go to Step 2.
 - b. Run the **display efm** command in the system view to check whether the EFM enable flag field is displayed as enabled.
 - If the EFM enable flag field is displayed as enabled, recheck the physical link and then check whether the alarm is cleared. If the alarm is not cleared, go to Step 3.
 - If EFM enable flag is not enabled, run the **efm enable** command in the system view and interface view according to the configuration guide. Then check whether the alarm is cleared. If the alarm persists, go to Step 3.
- 3. Collect alarm information and configuration information, and then contact technical support personnel.
- Cause 15: The tunnel is down.
 - a. Run the **display interface** command in the system view to check whether the tunnel link is Down.
 - If the physical status of the interface is Down, run the **undo shutdown** command to enable the interface and check whether the alarm is cleared. If the alarm persists, go to Step 2.

- If the physical status of the interface is Up, go to step 3.
 - b. Check whether the physical link is normal, for example, whether the network cable or optical module is loose or disconnected.
 - If the physical link is abnormal, reconnect the physical link and check whether the alarm is cleared. If the alarm persists, go to Step 3.
 - If the physical link works properly, go to Step 3.
 - c. Run the **display this** command in the interface view to check whether MPLS TE and MPLS RSVP-TE are configured on the tunnel interface and nodes.
 - If MPLS TE and MPLS RSVP-TE are configured on the tunnel link interface and node, go to Step 4.
 - If MPLS TE and MPLS RSVP-TE are not configured on the tunnel interface or node, run the **mpls te** and **mpls rsvp-te** commands in the MPLS view to reconfigure them. Then, check whether the alarm is cleared. If the alarm persists, go to Step 4.
 - d. Collect alarm and configuration information, and contact technical support personnel.
- Cause 16: The interface is shut down.
 - a. Run the **display this** command in the interface view to check whether the interfaces at both ends are shut down. If the interfaces are sub-interfaces, check whether VLAN IDs are configured for the interfaces at both ends.
 - If the interface is a sub-interface, run the **vlan-type dot1q** command to configure a correct VLAN ID for the sub-interface. Then, check whether the alarm is cleared. If the alarm persists, go to Step 2.
 - If the interface is not shut down, go to Step 2.
- 2. Collect alarm and configuration information, and contact technical support personnel.
- Cause 17: The link protocol is down.
 - a. Run the **display this** command in the interface view to check whether the interfaces at both ends are shut down. If the interfaces are sub-interfaces, check whether VLAN IDs are configured for the interfaces at both ends.
 - If the interface is a sub-interface, run the **vlan-type dot1q** command to configure a correct VLAN ID for the sub-interface. Then, check whether the alarm is cleared. If the alarm persists, go to Step 2.
 - If the interface is not shut down, go to Step 2.
 - b. Check the cause of the protocol Down event based on the corresponding link layer protocol.
 - If the link layer protocol can go Up, the fault is rectified.
 - If the link layer protocol still cannot go Up, go to Step 3.

- c. Collect alarm and configuration information, and contact technical support personnel.
- Cause 19: The link protocol is up.
This alarm message is informational only, and no action is required.
- Cause 20: The main interface is down.
 - a. Run the **display this** command in the interface view to check whether the interface on each end is shut down.
 - If the interface is shut down, run the **undo shutdown** command to enable the interface. After that, check whether the alarm is cleared. If the alarm is not cleared, go to Step 2.
 - If the interface is not shut down, go to Step 2.
 - b. Check whether the physical link of the interface works improperly. That is, check whether the hardware such as the network cable or optical module is disconnected or loosely connected.
 - If the physical link works improperly, you need to correctly connect the physical link and then check whether the alarm is cleared. If the alarm is not cleared, go to Step 3.
 - If the physical link works properly, go to Step 3.
- 3. Collect alarm information and configuration information, and then contact technical support personnel.
- Cause 21: Interface physical link is up.
This alarm message is informational only, and no action is required.
- Cause 22: The conditions for the activation of the interface are not met.
 - a. Run the **display interface** command in the system view to check whether the physical statuses of the local and remote interfaces are Up.
 - If physical statuses of the local and remote interfaces are Down, run the **undo shutdown** command in the interface view to enable the interface, and then check whether the alarm is cleared. If the alarm is not cleared, go to Step 2.
 - If physical statuses of the local and remote interfaces are Up, go to Step 2.
 - b. Run the **display eth-trunk** command in the system view to check whether the number of trunk member interfaces on the local and remote ends is larger than the max active-linkup number.
 - If the number is larger than the max active-linkup number, it indicates a normal situation in the LACP protocol negotiation process, and no action is required.
 - If the number is smaller than the max active-linkup number, go to Step 3.
 - c. Run the **display eth-trunk** command in the system view to check whether the number of trunk member interfaces on the local and remote ends is smaller than least active-linkup number.

- If the number of trunk member interfaces on the local and remote ends is less than least active-linkup number, run the **least active-linknumber** command to change least active-linkup number so that the former is greater than or equal to the latter.
 - If the number of trunk member interfaces on the local and remote ends is greater than least active-linkup number, go to Step 4.
4. Collect alarm information and configuration information, and then contact technical support personnel.
- Cause 23: The conditions for the activation of the interface are met.
This alarm message is informational only, and no action is required.
 - Cause 24: The tunnel is up.
This alarm message is informational only, and no action is required.
 - Cause 25: The interface is deleted.
Usually, it was because a user had deleted a logical interface. This alarm message is informational only, and no action is required.
 - Cause 26: BFD session is down.
 - a. Run the **display bfd session** command in the system view to check BFD session information.
 - If the interface is bound to a BFD session and the BFD session is in the Down state, refer to the BFD troubleshooting guide and rectify the fault.
 - If the interface is bound to a BFD session and the BFD session is in the Up state, go to Step 2.
2. Collect alarm information and configuration information, and then contact technical support personnel.
- Cause 27: BFD session is up.
This alarm message is informational only, and no action is required.
 - Cause 28: EFM UP.
This alarm message is informational only, and no action is required.
 - Cause 30: DLDP detect down.
 - a. Check the traps to determine the fault cause.
 - b. Check the possible causes.
 - Cause 31: DLDP detect up.
This alarm message is informational only, and no action is required.
 - Cause 32: VRRP FLOW DOWN.
 - a. Run the **display vrrp** command in the system view to check VRRP information.
 - If the mVRRP backup group is Down, refer to the VRRP troubleshooting guide and rectify the fault.
 - If the mVRRP backup group is Up, go to Step 2.
 - b. Collect alarm information and configuration information, and then contact technical support personnel.

- Cause 33: VRRP FLOW UP.
This alarm message is informational only, and no action is required.
- Cause 34: VE FLOW DOWN.
 - a. Run the **display interface virtual-ethernet ve-number** command to check VE interface information.
 - If the VE interface is Down, go to Step 2.
 - If the VE interface is Up, go to Step 4.
 - b. Collect the main interface configuration.
 - If it matches the L2VPN termination interface, see the L2VPN troubleshooting guide and rectify the fault.
 - If it matches the L3VPN termination interface, go to Step 3.
 - c. Collect the L3VPN termination sub-interface configuration, and check whether the sub-interface has a VLAN ID and IPv4 address configured.
 - If the configuration is not correct, go to Step 4.
 - If the configuration is correct but the alarm persists, go to Step 4.
 - d. Collect alarm information and configuration information, and then contact technical support personnel.
- Cause 35: VE FLOW UP.
This alarm message is informational only, and no action is required.
- Cause 36: The interface is error down.
For details about handling suggestions, see "ERROR-DOWN_1.3.6.1.4.1.2011.5.25.257.2.1 hwErrordown" Handling Procedure.
- Cause 37: CRC ERR DOWN.
 - a. Run the **display interface [interface-type [interface-number] | slot slot-number]** command to check the status of the link layer protocol on the interface.
 - If the status of the link layer protocol on the interfaces is Up (Bit-error-detection down), BER exceeds the BER alarm threshold, go to Step 2.
 - If the status of the link layer protocol on the interfaces is Down (Bit-error-detection down), go to Step 3.
 - b. Check whether the physical link of the interface works improperly. That is, check whether the hardware such as the network cable or optical module is disconnected or loosely connected.
 - If the physical link works improperly, you need to correctly connect the physical link and then check whether the alarm is cleared. If the alarm is not cleared, go to Step 3.
 - If the physical link works properly, go to Step 3.
 - c. Collect alarm information and configuration information, and then contact technical support personnel.

- Cause 38: CRC ERR UP.
This alarm message is informational only, and no action is required.
- Cause 39: Transceiver speed does not match the speed configured on the port.
 - a. Delete the speed configuration on the port and check whether the alarm is cleared. If the alarm persists, go to Step 2.
 - b. Check whether the physical link of the interface works improperly. That is, check whether the hardware such as the network cable or optical module is disconnected or loosely connected.
 - If the physical link works improperly, you need to correctly connect the physical link and then check whether the alarm is cleared. If the alarm is not cleared, go to Step 3.
 - If the physical link works properly, go to Step 3.
 - c. Collect alarm information and configuration information, and then contact technical support personnel.
- Cause 40: The port does not support current transceiver.
 - a. Replace the current transceiver with a transceiver that the port supports and check whether the alarm is cleared. If the alarm persists, go to Step 2.
 - b. Check whether the physical link of the interface works improperly. That is, check whether the hardware such as the network cable or optical module is disconnected or loosely connected.
 - If the physical link works improperly, you need to correctly connect the physical link and then check whether the alarm is cleared. If the alarm is not cleared, go to Step 3.
 - If the physical link works properly, go to Step 3.
 - c. Collect alarm information and configuration information, and then contact technical support personnel.
- Cause 41: Transceiver does not support the negotiation configuration on the port.
 - a. Delete the negotiation configuration on the port and check whether the alarm is cleared. If the alarm persists, go to Step 2.
 - b. Check whether the physical link of the interface works improperly. That is, check whether the hardware such as the network cable or optical module is disconnected or loosely connected.
 - If the physical link works improperly, you need to correctly connect the physical link and then check whether the alarm is cleared. If the alarm is not cleared, go to Step 3.
 - If the physical link works properly, go to Step 3.
 - c. Collect alarm information and configuration information, and then contact technical support personnel.
- Cause 43: The interface is trigger down.
 - a. Run the **display interface [interface-type [interface-number] | slot slot-number]** command and check whether the specified interface status is TRIGGER DOWN.

- If the interface status is TRIGGER DOWN, go to Step 2.
 - If the interface status is not TRIGGER DOWN, go to Step 4.
 - b. Check the cause following the TRIGGER DOWN field and view the associated service, for example, TRIGGER DOWN (MONITOR GROUP).
 - If a cause is displayed, go to Step 3.
 - If no cause is displayed, go to Step 4.
 - c. Check and restore the associated service. Check whether the trap is cleared. If the trap persists, go to Step 4.
 - d. Collect alarm information and configuration information, and then contact technical support personnel.
- Cause 48: CFM DOWN.
 - a. Check the CFM status information.
 - If the CFM status is normal, go to Step 2.
 - If the CFM status is abnormal, see CFM-related troubleshooting.
 - b. Please Collect alarm information and configuration information, and then contact technical support personnel.
- Cause 49: CFM UP.

This alarm message is informational only, and no action is required.
- Cause 51: The sub-interface linkDown alarm is disabled.

This alarm message is informational only, and no action is required.

3.5.5.12 ALM-135463100 hwIfMonitorCrcErrorRising

Description

The CRC error is rising. (hwIfMonitorIndex=[EntityPhysicalIndex], hwIfMonitorCrcErrorStatistics=[hwIfMonitorCrcErrorStatistics], hwIfMonitorCrcErrorThreshold=[hwIfMonitorCrcErrorThreshold], hwIfMonitorCrcErrorInterval=[hwIfMonitorCrcErrorInterval], EntPhysicalName=[EntPhysicalName], hwIfMonitorAllStatistics=[hwIfMonitorAllStatistics])

The number of CRC error packets received by the interface in a specified period exceeded the upper threshold.

Attribute

AlarmID	Alarm OID	Alarm Severity	Alarm Type
135463100	1.3.6.1.4.1.2011.5.25.41.4.1	Critical	Processing error alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
EntityPhysicalIndex	Entity index.
hwIfMonitorCrcErrorStatistics	Real-time statistics of CRC error packets
hwIfMonitorCrcErrorThreshold	Upper threshold for the number of CRC error packets
hwIfMonitorCrcErrorInterval	Configured statistics collection interval
EntPhysicalName	Entity name
hwIfMonitorAllStatistics	Number of packets in real-time statistics

Impact on the System

An interface receives a large number of CRC error packets, which may cause the interface to transit to the Error-Down state.

Possible Causes

The interface receives excessive CRC error packets whose lengths are greater than or equal to 64 bytes in a specified period of time.

Procedure

1. Run the **display this** command in the interface view to check whether the alarm threshold for error packets is too low.Determine the alarm threshold based on service requirements.
 - If so, go to Step 2.
 - If no, go to Step 3.
2. Run the **trap-threshold crc-statistics** command in the interface view to set a larger alarm threshold for error packets. Then check whether the alarm is cleared.
 - If yes, no further action is required.
 - If no, go to Step 3.
3. Collect trap, log, and configuration information, and contact technical support personnel.

3.5.5.13 ALM-15795032 hwStorageUtilizationRisingAlarm

Description

The storage usage exceeded the pre-set overload threshold.
(TrapSeverity=[TrapSeverity], ProbableCause=[ProbableCause],
EventType=[EventType], PhysicalIndex=[PhysicalIndex],
PhysicalName=[PhysicalName], RelativeResource=[RelativeResource],
UsageType=[UsageType], SubIndex=[SubIndex], UsageValue=[UsageValue],
Unit=[Unit], UsageThreshold=[UsageThreshold])

Memory or storage usage was sampled for a period of time. In one sampling period (overload times x sampling interval), if each memory or storage usage sample exceeded the pre-set overload threshold, this alarm was generated.

Attribute

Alarm ID	OID	Alarm Severity	Alarm Type
15795032	1.3.6.1.4.1.2011.5.25.129.2.6.1	Major	Quality of service alarm

Parameters

Name	Meaning
TrapSeverity	Alarm severity.
ProbableCause	Possible cause, values are as follows: 75264: Memory usage exceeded the overload threshold. 75265: Storage usage exceeded the overload threshold. 75275: The log partition usage exceeded the pre-set overload threshold.
EventType	Alarm type.
PhysicalIndex	Physical index.
PhysicalName	Entity name.
RelativeResource	Relevant resource name.

Name	Meaning
UsageType	Overload type.1 indicates the CPU, 2 indicates the memory, 3 indicates the disk, 4 indicates the flash memory, 5 indicates the CF card, and 6 indicates the physical memory.
SubIndex	Entity sub-index.
UsageValue	Storage usage.
Unit	Unit.
UsageThreshold	Overload threshold.

Impact on the System

- Cause 75264: The memory usage exceeded the pre-set overload threshold.
If services cannot successfully obtain memory resources, the system automatically restarts.
- Cause 75265: The storage usage exceeded the pre-set overload threshold.
If the remaining space in the storage medium is insufficient, the log function and software upgrade are affected.
- Cause 75275: The log partition usage exceeded the pre-set overload threshold.
If the storage space of the log partition is insufficient, the log function is affected.

Possible Causes

- Cause 75264: The memory usage exceeded the pre-set overload threshold.
- Cause 75265: The storage usage exceeded the pre-set overload threshold.
- Cause 75275: The log partition usage exceeded the pre-set overload threshold.

Procedure

- Cause 75264: The memory usage exceeded the pre-set overload threshold.
 - a. Run the **display system memory statistics** command to view the memory usage, and run the **display memory threshold** command to view the overload threshold.
 - If the memory usage exceeded the overload threshold, go to Step 2.
 - If the memory usage is below the overload threshold, go to Step 4.
 - b. Reduce unnecessary services or delete unnecessary configurations to reduce the memory usage, and then check whether this alarm is cleared.

- When deleting service configurations, submit 3~5 configurations at a time.
- If this alarm is cleared, it indicates that the problem is solved.
 - If this alarm persists, go to Step 3.
- c. Run the **set memory threshold** command to change the overload threshold, and then check whether this alarm is cleared.
- If this alarm is cleared, it indicates that the problem is solved.
 - If this alarm persists, go to Step 4.
4. Collect the alarm information, log information, and configuration information, and contact Huawei technical support engineers.
- Cause 75265: The storage usage exceeded the pre-set overload threshold.
 - a. Run the **cd** command to access the directory, and run the **dir** command to view the storage usage.
 - If the storage usage exceeded the overload threshold, go to Step 2.
 - If the storage usage is below the overload threshold, go to Step 3.
 - b. Delete unnecessary files to reduce the storage usage.
 - If this alarm is cleared, it indicates that the problem is solved.
 - If this alarm persists, go to Step 3.
 - c. Collect the alarm information, log information, and configuration information, and contact technical support engineers.
 - Cause 75275: The log partition usage exceeded the pre-set overload threshold.

Delete unnecessary logs to reduce the log partition usage. Then, check whether the alarm is cleared.

3.5.5.14 ALM-135462996 hwBoardFail

Description

The board partially failed. (EntPhysicalIndex=[EntPhysicalIndex], EntPhysicalName=[EntPhysicalName], EntityType=[EntityType], EntityTrapFaultID=[EntityTrapFaultID], Reason=[Reason])

The card experienced a partial failure.

Attribute

AlarmID	Alarm OID	Alarm Severity	Alarm Type
135462996	1.3.6.1.4.1.2011.5.25.219.2.2.3	Critical	Equipment alarm

Parameters

Name	Meaning
EntPhysicalIndex	Entity index.
EntPhysicalName	Entity name.
EntityType	Entity type.
EntityTrapFaultID	Alarm cause.
Reason	

Impact on the System

- Cause 1: Power supply abnormal.
Services on the card may be affected or even interrupted.
- Cause 2: A voltage drop occurred on the board.
Services on the card may be affected or even interrupted.
- Cause 3: The serial management bus of the board malfunctions.
Services on the card may be affected or even interrupted.
- Cause 6: Board RTC fault.
Services on the card may be affected or even interrupted.
- Cause 8: The fan is not full.
As a result, fan information cannot be obtained.
- Cause 11: A data channel fault occurred on the forwarding engine.
Services on the card may be affected or even interrupted.
- Cause 12: The forwarding engine failed.
Services on the card may be affected or even interrupted.
- Cause 13: Inter-card broadcast traffic failed to be forwarded.
Services on the card may be affected or even interrupted.
- Cause 15: Fabric interface input or output bandwidth usage exceeded 90% continuously.
Services on the card may be affected or even interrupted.
- Cause 16: Ingress clock signals channel failed.
Services on the card may be affected or even interrupted.
- Cause 17: The sensor on the board was faulty.
Services on the card may be affected or even interrupted.
- Cause 18: Chip instability.
Services on the card may be affected or even interrupted.
- Cause 19: Egress clock signals channel failed.
Services on the card may be affected or even interrupted.
- Cause 20: A packet reassembly error occurred.
Services on the card may be affected or even interrupted.

- Cause 21: Board CANBUS failed.
Services on the card may be affected or even interrupted.
- Cause 23: Board cannot be powered on or powered off properly.
Services on the card may be affected or even interrupted.
- Cause 24: EEPROM is abnormal.
The current services are not affected, but the services after the next startup of the board are affected.
- Cause 25: The fan model does not match the device.
Services on the card may be affected or even interrupted.
- Cause 26: The power supply model does not match the device.
Services on the card may be affected or even interrupted.
- Cause 27: The PHY chip is abnormal.
Services on the card may be affected or even interrupted.
- Cause 29: Board PLL instability.
Services on the card may be affected or even interrupted.
- Cause 30: Phy instability.
Services on the card may be affected or even interrupted.
- Cause 36: USB overcurrent occurred.
Services on the card may be affected or even interrupted.
- Cause 37: IIC failed.
Services on the card may be affected or even interrupted.
- Cause 38: LANSWITCH chip instability.
Services on the card may be affected or even interrupted.
- Cause 39: The link of the XFI interface is faulty.
Services on the card may be affected or even interrupted.
- Cause 40: A CRC error occurred on the XFI interface.
Services on the card may be affected or even interrupted.
- Cause 43: The memory size is different from the standard configuration.
Services on the card may be affected or even interrupted.
- Cause 44: Flash memory failed.
Services on the card may be affected or even interrupted.
- Cause 50: CMU on the MPU is not registered.
Services on the card may be affected or even interrupted.
- Cause 51: The 38M clock fails.
Services on the card may be affected or even interrupted.
- Cause 52: The 19M clock fails.
Services on the card may be affected or even interrupted.
- Cause 53: The board clock fails.
Services on the card may be affected or even interrupted.
- Cause 54: The PLLA inside the forwarding engine is not ready.
Services on the card may be affected or even interrupted.

- Cause 55: The Serdes on the board failed.
Services on the card may be affected or even interrupted.
- Cause 56: An internal modular of the forwarding engine is abnormal.
Services on the card may be affected or even interrupted.
- Cause 58: The active and standby MPUs cannot communicate with each other.
Services on the card may be affected or even interrupted.
- Cause 59: The board type cannot be identified.
Services on the card may be affected or even interrupted.
- Cause 60: The board clock(156M) failed.
Services on the card may be affected or even interrupted.
- Cause 65: Storage media is abnormal.
Services on the card may be affected or even interrupted.
- Cause 70: CANBUS communications between the monitor chips failed.
Services on the card may be affected or even interrupted.
- Cause 71: A DDR fault occurs on the board.
Services on the card may be affected or even interrupted.
- Cause 72: The slot ID of the board fails to be checked.
Services on the card may be affected or even interrupted.
- Cause 73: Access to the flash memory of the board fails.
Services on the card may be affected or even interrupted.
- Cause 74: The FULLIN signal of the board is abnormal.
Services on the card may be affected or even interrupted.
- Cause 75: The slot ID signal from the CANBUS is abnormal.
Services on the card may be affected or even interrupted.
- Cause 76: A SerialCpldLocalbus fault occurs on the board.
Services on the card may be affected or even interrupted.
- Cause 77: The micro switch of the board fails.
Services on the card may be affected or even interrupted.
- Cause 78: The frequency synthesizer failed.
Services on the card may be affected or even interrupted.
- Cause 80: A CPU fault occurred.
Services on the card may be affected or even interrupted.
- Cause 82: A CPU-side CRC fault occurred.
Services on the card may be affected or even interrupted.
- Cause 83: A PHY-side CRC fault occurred.
Services on the card may be affected or even interrupted.
- Cause 84: The disk will soon become invalid.
Services on the card may be affected or even interrupted.
- Cause 88: The Chip is failed.
Services on the card may be affected or even interrupted.

- Cause 90: Overcurrent occurred on the board.
Services on the card may be affected or even interrupted.
- Cause 91: The FPGA is abnormal.
Services on the card may be affected or even interrupted.
- Cause 92: The sensor chip on the board was faulty.
Services on the card may be affected or even interrupted.
- Cause 96: A HTM chip fault occurred.
Services on the card may be affected or even interrupted.
- Cause 99: Failed to check the voltage of the board.
Services on the card may be affected or even interrupted.
- Cause 102: The currently used hard disk is not certified by Huawei.
Services on the card may be affected or even interrupted.
- Cause 103: The hard disk was pulled out.
Services on the card may be affected or even interrupted.
- Cause 104: The device certificate verification failed.
The key components of the board may have been replaced, which affects system reliability and security.
- Cause 105: Failed to access backplane IIC.
Services on the card may be affected or even interrupted.
- Cause 106: Failed to check backplane ID.
Services on the card may be affected or even interrupted.
- Cause 107: The IIC of MCU module is abnormal.
Services on the card may be affected or even interrupted.

Possible Causes

- Cause 1: Power supply abnormal.
- Cause 2: A voltage drop occurred on the board.
- Cause 3: The serial management bus of the board malfunctions.
- Cause 6: Board RTC fault.
- Cause 8: The fan is not full.
- Cause 11: A data channel fault occurred on the forwarding engine.
- Cause 12: The forwarding engine failed.
- Cause 13: Inter-card broadcast traffic failed to be forwarded.
- Cause 15: Fabric interface input or output bandwidth usage exceeded 90% continuously.
- Cause 16: Ingress clock signals channel failed.
- Cause 17: The sensor on the board was faulty.
- Cause 18: Chip instability.
- Cause 19: Egress clock signals channel failed.
- Cause 20: A packet reassembly error occurred.
- Cause 21: Board CANBUS failed.

- Cause 23: Board cannot be powered on or powered off properly.
- Cause 24: EEPROM is abnormal.
- Cause 25: The fan model does not match the device.
- Cause 26: The power supply model does not match the device.
- Cause 27: The PHY chip is abnormal.
- Cause 29: Board PLL instability.
- Cause 30: Phy instability.
- Cause 36: USB overcurrent occurred.
- Cause 37: IIC failed.
- Cause 38: LANSWITCH chip instability.
- Cause 39: The link of the XFI interface is faulty.
- Cause 40: A CRC error occurred on the XFI interface.
- Cause 43: The memory size is different from the standard configuration.
- Cause 44: Flash memory failed.
- Cause 50: CMU on the MPU is not registered.
- Cause 51: The 38M clock fails.
- Cause 52: The 19M clock fails.
- Cause 53: The board clock fails.
- Cause 54: The PLLA inside the forwarding engine is not ready.
- Cause 55: The Serdes on the board failed.
- Cause 56: An internal modular of the forwarding engine is abnormal.
- Cause 58: The active and standby MPUs cannot communicate with each other.
- Cause 59: The board type cannot be identified.
- Cause 60: The board clock(156M) failed.
- Cause 65: Storage media is abnormal.
- Cause 70: CANBUS communications between the monitor chips failed.
- Cause 71: A DDR fault occurs on the board.
- Cause 72: The slot ID of the board fails to be checked.
- Cause 73: Access to the flash memory of the board fails.
- Cause 74: The FULLIN signal of the board is abnormal.
- Cause 75: The slot ID signal from the CANBUS is abnormal.
- Cause 76: A SerialCpldLocalbus fault occurs on the board.
- Cause 77: The micro switch of the board fails.
- Cause 78: The frequency synthesizer failed.
- Cause 80: A CPU fault occurred.
- Cause 82: A CPU-side CRC fault occurred.
- Cause 83: A PHY-side CRC fault occurred.
- Cause 84: The disk will soon become invalid.
- Cause 88: The Chip is failed.
- Cause 90: Overcurrent occurred on the board.

- Cause 91: The FPGA is abnormal.
- Cause 92: The sensor chip on the board was faulty.
- Cause 96: A HTM chip fault occurred.
- Cause 99: Failed to check the voltage of the board.
- Cause 102: The currently used hard disk is not certified by Huawei.
- Cause 103: The hard disk was pulled out.
- Cause 104: The device certificate verification failed.
- Cause 105: Failed to access backplane IIC.
- Cause 106: Failed to check backplane ID.
- Cause 107: The IIC of MCU module is abnormal.

Procedure

- Cause 1: Power supply abnormal.
 1. If the faulty board is not reset or powered off and services are running properly, go to step 3.
 2. Power off and then power on the faulty board. If the fault persists, go to step 3.
 3. Collect trap, log, and configuration information, and contact technical support personnel.
- Cause 2: A voltage drop occurred on the board.
 1. Collect alarm, log, and configuration information, and contact technical support personnel.
- Cause 3: The serial management bus of the board malfunctions.
 1. Collect alarm, log, and configuration information, and contact technical support personnel.
- Cause 6: Board RTC fault.
 1. If the faulty board is not reset or powered off and services are running properly, go to step 3.
 2. Power off and then power on the faulty board. If the fault persists, go to step 3.
 3. Collect trap, log, and configuration information, and contact technical support personnel.
- Cause 8: The fan is not full.

Insert the fan module into the corresponding slot.
- Cause 11: A data channel fault occurred on the forwarding engine.
 1. Reset the board. If the fault persists, go to step 2.
 2. Collect trap, log, and configuration information, and contact technical support personnel.
- Cause 12: The forwarding engine failed.
 1. Reset the board. If the fault persists, go to step 2.
 2. Collect trap, log, and configuration information, and contact technical support personnel.
- Cause 13: Inter-card broadcast traffic failed to be forwarded.

1. Collect alarm and log information, and contact technical support personnel.
- Cause 15: Fabric interface input or output bandwidth usage exceeded 90% continuously.
 1. Collect alarm and log information, and contact technical support personnel.
- Cause 16: Ingress clock signals channel failed.
 1. Collect alarm and log information, and contact technical support personnel.
- Cause 17: The sensor on the board was faulty.
 1. Reset the board. If the fault persists, go to step 2.
 2. Collect trap, log, and configuration information, and contact technical support personnel.
- Cause 18: Chip instability.
 1. Reset the board. If the fault persists, go to step 2.
 2. Collect trap, log, and configuration information, and contact technical support personnel.
- Cause 19: Egress clock signals channel failed.
 1. Collect alarm and log information, and contact technical support personnel.
- Cause 20: A packet reassembly error occurred.
 1. Collect alarm and log information, and contact technical support personnel.
- Cause 21: Board CANBUS failed.
 1. Reset the faulty board. If the fault persists, go to step 2.
 2. Collect trap, log, and configuration information, and contact technical support personnel.
- Cause 23: Board cannot be powered on or powered off properly.
 1. Power off and then power on the faulty board. If the fault persists, go to step 2.
 2. Collect trap, log, and configuration information, and contact technical support personnel.
- Cause 24: EEPROM is abnormal.
 1. Check whether the services on the board are normal.
 - If so, go to step 4.
 - If not, go to step 2.
 2. Securely insert the board, and then check whether the alarm is cleared.
 - If so, go to step 5.
 - If not, go to step 3.
 3. Replace the faulty board, and then check whether the alarm is cleared.
 - If so, go to step 5.
 - If not, go to step 4.
 4. Collect alarm, log, and configuration information, and contact technical support engineers.
 5. End.
- Cause 25: The fan model does not match the device.
 1. Replace the fan module with one that matches the device model.

- Cause 26: The power supply model does not match the device.
 1. Replace the fan or power module with a new one that matches the device model.
- Cause 27: The PHY chip is abnormal.
 1. Collect alarm, log, and configuration information, and contact technical support personnel.
- Cause 29: Board PLL instability.
 1. Reset and restart the system.
 2. If the fault persists, replace the board.
- Cause 30: Phy instability.
 1. If the faulty board is not reset or powered off and services are running properly, go to step 3.
 2. Power off and then power on the faulty board. If the fault persists, go to step 3.
 3. Collect trap, log, and configuration information, and contact technical support personnel.
- Cause 36: USB overcurrent occurred.
 1. Collect alarm, log, and configuration information, and contact technical support personnel.
- Cause 37: IIC failed.
 1. Collect alarm, log, and configuration information, and contact technical support personnel.
- Cause 38: LANSWITCH chip instability.
 1. Reset the board. If the fault persists, go to step 2.
 2. Collect trap, log, and configuration information, and contact technical support personnel.
- Cause 39: The link of the XFI interface is faulty.
 1. Collect alarm, log, and configuration information, and contact technical support personnel.
- Cause 40: A CRC error occurred on the XFI interface.
 1. Collect alarm, log, and configuration information, and contact technical support personnel.
- Cause 43: The memory size is different from the standard configuration.
 1. Run the display version command to check whether the board memory meets the specifications. If the board memory does not meet the specifications, contact technical support personnel.
- Cause 44: Flash memory failed.
 1. Reset the board. If the fault persists, go to step 2.
 2. Collect trap, log, and configuration information, and contact technical support personnel.
- Cause 50: CMU on the MPU is not registered.

Collect alarm, log, and configuration information and contact Huawei technical support.
- Cause 51: The 38M clock fails.

1. Collect alarm, log, and configuration information, and contact technical support personnel.
- Cause 52: The 19M clock fails.
Collect alarm, log, and configuration information and contact Huawei technical support.
- Cause 53: The board clock fails.
1. Collect alarm, log, and configuration information, and contact technical support personnel.
- Cause 54: The PLLA inside the forwarding engine is not ready.
1. Collect alarm, log, and configuration information, and contact technical support personnel.
- Cause 55: The Serdes on the board failed.
1. Reset the board. If the fault persists, go to step 2.
2. Collect trap, log, and configuration information, and contact technical support personnel.
- Cause 56: An internal modular of the forwarding engine is abnormal.
1. Collect alarm, log, and configuration information, and contact technical support personnel.
- Cause 58: The active and standby MPUs cannot communicate with each other.
1. Collect alarm, log, and configuration information, and contact technical support personnel.
- Cause 59: The board type cannot be identified.
1. Collect alarm and log information, and contact technical support personnel.
- Cause 60: The board clock(156M) failed.
Collect alarm and log information and contact Huawei technical support.
- Cause 65: Storage media is abnormal.
1. Collect alarm, log, and configuration information, and contact technical support personnel.
- Cause 70: CANBUS communications between the monitor chips failed.
1. Collect alarm, log, and configuration information, and contact technical support personnel.
- Cause 71: A DDR fault occurs on the board.
1. Collect alarm, log, and configuration information, and contact technical support personnel.
- Cause 72: The slot ID of the board fails to be checked.
1. Collect alarm, log, and configuration information, and contact technical support personnel.
- Cause 73: Access to the flash memory of the board fails.
1. Collect alarm, log, and configuration information, and contact technical support personnel.
- Cause 74: The FULLIN signal of the board is abnormal.
1. Collect alarm, log, and configuration information, and contact technical support personnel.

- Cause 75: The slot ID signal from the CANBUS is abnormal.
1. Collect alarm, log, and configuration information, and contact technical support personnel.
- Cause 76: A SerialCpldLocalbus fault occurs on the board.
1. Collect alarm, log, and configuration information, and contact technical support personnel.
- Cause 77: The micro switch of the board fails.
1. Collect alarm, log, and configuration information, and contact technical support personnel.
- Cause 78: The frequency synthesizer failed.
1. Collect alarm, log, and configuration information, and contact technical support personnel.
- Cause 80: A CPU fault occurred.
1. Collect alarm, log, and configuration information, and contact technical support personnel.
- Cause 82: A CPU-side CRC fault occurred.
1. Collect alarm, log, and configuration information, and contact technical support personnel.
- Cause 83: A PHY-side CRC fault occurred.
1. Collect alarm, log, and configuration information, and contact technical support personnel.
- Cause 84: The disk will soon become invalid.
1. Collect alarm, log, and configuration information, and contact technical support personnel.
- Cause 88: The Chip is failed.
1. Collect alarm, log, and configuration information, and contact technical support personnel.
- Cause 90: Overcurrent occurred on the board.
1. Collect alarm, log, and configuration information, and contact technical support personnel.
- Cause 91: The FPGA is abnormal.
1. Collect alarm, log, and configuration information, and contact technical support personnel.
- Cause 92: The sensor chip on the board was faulty.
1. Collect alarm, log, and configuration information, and contact technical support personnel.
- Cause 96: A HTM chip fault occurred.
1. Collect alarm, log, and configuration information, and contact technical support personnel.
- Cause 99: Failed to check the voltage of the board.
1. Collect alarm, log, and configuration information, and contact technical support personnel.
- Cause 102: The currently used hard disk is not certified by Huawei.
Remove non-Huawei-certified hard disks and insert Huawei-certified hard disks.

- Cause 103: The hard disk was pulled out.
Insert a hard disk.
- Cause 104: The device certificate verification failed.
Reset the board and check whether the fault is rectified. If the fault persists, replace the board.
- Cause 105: Failed to access backplane IIC.
Collect alarm, log, and configuration information and contact Huawei technical support.
- Cause 106: Failed to check backplane ID.
Collect alarm, log, and configuration information and contact Huawei technical support.
- Cause 107: The IIC of MCU module is abnormal.
Collect alarm, log, and configuration information and contact Huawei technical support.

Related Information

None.

3.5.5.15 ALM-135462925 hwBrdTempAlarm

Description

The board temperature exceeded the upper alarm threshold.
(EntPhysicalIndex=[EntPhysicalIndex], EntPhysicalName=[EntPhysicalName], EntityThresholdType=[EntityThresholdType], EntityThresholdWarning=[EntityThresholdWarning], EntityThresholdCurrent=[EntityThresholdCurrent], EntityTrapFaultID=[EntityTrapFaultID], Reason=[ReasonDsp])

The board or card temperature was too high.

Attribute

Alarm ID	OID	Alarm Severity	Alarm Type
135462925	1.3.6.1.4.1.2011.5.25.219.2.10.13	Minor	Environmental alarm

Parameters

Name	Meaning
EntPhysicalIndex	Indicates the index of an entity.
EntPhysicalName	Indicates the name of an entity.

Name	Meaning
EntityThresholdType	Indicates the threshold type of the entity.
EntityThresholdWarning	Indicates the temperature threshold of the entity.
EntityThresholdCurrent	Indicates the current temperature.
EntityTrapFaultID	Indicates the error code.
ReasonDsp	Indicates a possible cause.

Impact on the System

- Cause 1: Services are not affected temporarily, but the subcard temperature needs to be lowered as soon as possible.
- Cause 2: Services are not affected temporarily, but the board temperature needs to be lowered as soon as possible.
- Cause 3: Services are not affected temporarily, but the board temperature needs to be increased as soon as possible.
- Cause 4: Services are not affected temporarily, but the subcard temperature needs to be increased as soon as possible.

Possible Causes

- Cause 1: The card temperature was too high.
- Cause 2: The board temperature was too high.
- Cause 3: The board temperature fell below the lower limit.
- Cause 4: The subcard temperature fell below the lower limit.

Procedure

- Cause 1: The card temperature was too high.
 - a. Check whether the air filter of the fan is blocked.
 - If so, clean the air filter.
 - If not, go to step 2.
 - b. Check whether the ambient temperature is too high.
 - If so, reduce the ambient temperature.
 - If not, go to step 3.
 - c. Check whether the fan is faulty.
 - If so, rectify the fan fault.

- If not, go to step 4.
 - d. Check whether a filler panel is installed in the slot that has no subcard installed.
 - If so, go to step 5.
 - If not, install a filler panel in the slot.
 - e. Collect traps, logs, and configurations, and contact technical support personnel.
- Cause 2: The board temperature was too high.
 - a. Check whether the air filter of the fan is blocked.
 - If so, clean the air filter.
 - If not, go to step 2.
 - b. Check whether the ambient temperature is too high.
 - If so, reduce the ambient temperature.
 - If not, go to step 3.
 - c. Check whether the fan is faulty.
 - If so, rectify the fan fault.
 - If not, go to step 4.
 - d. Check whether a filler panel is installed in the slot that has no board installed.
 - If so, go to step 5.
 - If not, install a filler panel in the slot.
 - e. Collect traps, logs, and configurations, and contact technical support personnel.
- Cause 3: The board temperature fell below the lower limit.
 - a. Adjust the ambient temperature or increase the distance between the device and the air conditioner.
 - b. Collect trap, log, and configuration information, and contact Huawei technical support personnel.
- Cause 4: The subcard temperature fell below the lower limit.
 - a. Adjust the ambient temperature or increase the distance between the device and the air conditioner. Collect trap, log, and configuration information, and contact Huawei technical support personnel.

3.5.5.16 ALM-135463001 hwOpticalInvalid

Description

Optical Module is invalid. (EntPhysicalIndex=[EntPhysicalIndex], EntPhysicalName=[EntPhysicalName], EntityTrapFaultID=[EntityTrapFaultID], Reason=[Reason])

An optical module was faulty.

Attribute

AlarmID	Alarm OID	Alarm Severity	Alarm Type
135463001	1.3.6.1.4.1.2011.5.25 .219.2.4.5	Minor	Equipment alarm

Parameters

Parameter	Description
EntPhysicalIndex	Entity index.
EntPhysicalName	Entity name.
EntityTrapFaultID	Alarm cause.
Reason	

Impact on the System

- Cause 2: Output Optical Power Too High.
Services on the optical module may be affected, which may cause bit errors, error packets, or even service interruption.
- Cause 3: Output Optical Power Too Low.
Services on the optical module may be affected, which may cause bit errors, error packets, or even service interruption.
- Cause 4: Input Optical Power Too High.
Services on the optical module may be affected, which may cause bit errors, error packets, or even service interruption.
- Cause 5: Input Optical Power Too Low.
Services on the optical module may be affected, which may cause bit errors, error packets, or even service interruption.
- Cause 7: The IIC of the optical module failed.
Services on the optical module may be affected, which may cause bit errors, error packets, or even service interruption.
- Cause 8: The optical signals received by the optical module were lost.
Services on the optical module may be affected, which may cause bit errors, error packets, or even service interruption.
- Cause 9: The electrical signals sent by the optical module were lost.
Services on the optical module may be affected, which may cause bit errors, error packets, or even service interruption.
- Cause 10: Loss of lock was detected in the receive direction by the optical module.

Services on the optical module may be affected, which may cause bit errors, error packets, or even service interruption.

- Cause 11: Loss of lock was detected in the transmit direction by the optical module.

Services on the optical module may be affected, which may cause bit errors, error packets, or even service interruption.

- Cause 12: The optical module failed to send signals.

Services on the optical module may be affected, which may cause bit errors, error packets, or even service interruption.

- Cause 13: The voltage of the optical module was too high.

Services may be interrupted.

- Cause 14: The voltage of the optical module was too low.

Services may be interrupted.

- Cause 15: The bias current of the optical module was too high.

Services may be interrupted.

- Cause 16: The bias current of the optical module was too low.

Services may be interrupted.

- Cause 17: The temperature of the optical module was too high.

Services may be interrupted.

- Cause 18: The temperature of the optical module was too low.

Services may be interrupted.

- Cause 19: The power current of the optical module is too high.

Services might be interrupted.

Possible Causes

- Cause 2: Output Optical Power Too High.
- Cause 3: Output Optical Power Too Low.
- Cause 4: Input Optical Power Too High.
- Cause 5: Input Optical Power Too Low.
- Cause 7: The IIC of the optical module failed.
- Cause 8: The optical signals received by the optical module were lost.
- Cause 9: The electrical signals sent by the optical module were lost.
- Cause 10: Loss of lock was detected in the receive direction by the optical module.
- Cause 11: Loss of lock was detected in the transmit direction by the optical module.
- Cause 12: The optical module failed to send signals.
- Cause 13: The voltage of the optical module was too high.
- Cause 14: The voltage of the optical module was too low.
- Cause 15: The bias current of the optical module was too high.
- Cause 16: The bias current of the optical module was too low.
- Cause 17: The temperature of the optical module was too high.

- Cause 18: The temperature of the optical module was too low.
- Cause 19: The power current of the optical module is too high.

Procedure

- Cause 2: Output Optical Power Too High.
 1. Run the display interface command in the user view to check whether the Tx power of the interface is within the allowed range.
 - If so, collect alarm, log, and configuration information, and contact technical support personnel.
 - If not, replace the optical module.
 2. If the alarm persists, collect alarm, log, and configuration information, and contact technical support personnel.
- Cause 3: Output Optical Power Too Low.
 1. Run the display interface command in the user view to check whether the Tx power of the interface is within the allowed range.
 - If so, go to step 2.
 - If not, replace the optical module.
 2. Collect alarm, log, and configuration information, and contact technical support personnel.
- Cause 4: Input Optical Power Too High.
 1. Run the display interface command in the user view to check whether the Rx power of the interface is within the allowed range.
 - If so, collect trap, log, and configuration information, and contact technical support personnel.
 - If not, go to step 2.
 2. Check whether an alarm indicating that the Tx power is too high is generated on the remote interface.
 - If so, clear the alarm on the remote interface first.
 - If not, go to step 3.
 3. Check whether the peer optical module matches the local optical module.
 - If not, replace the optical module with one that matches the peer optical module.
 - If so, go to step 4.
 4. Add an optical attenuator to the local end. It is recommended that the attenuation be increased by -5 dB.
 5. If the alarm persists, replace the optical module.
 6. If the alarm still persists, collect alarm, log, and configuration information, and contact technical support personnel.
- Cause 5: Input Optical Power Too Low.
 1. Run the display interface command in the user view to check whether the Rx power of the interface is within the allowed range.
 - If so, collect trap, log, and configuration information, and contact technical support personnel.
 - If not, go to step 2.

2. If the peer interface is not Down and no alarm is generated, go to step 4.
 3. Rectify the fault and clear the alarm on the peer interface. If the alarm is cleared, no further action is required.
 4. Check whether the optical fiber is faulty. If so, replace the optical fiber.
 5. Check whether an alarm is generated on the local interface. If so, replace the optical module to rectify the fault.
 6. If the alarm persists after the optical module is replaced, collect alarm, log, and configuration information, and contact technical support personnel.
- Cause 7: The IIC of the optical module failed.
 1. Check whether the optical module is securely installed. If so, remove the optical module and check whether the port has bent pins or is damaged. Try replacing the optical module. If the fault persists, contact technical support personnel.
 - Cause 8: The optical signals received by the optical module were lost.

Check whether the optical fiber is faulty. If so, replace the optical fiber. If the fault persists, collect alarm, log, and configuration information, and contact technical support personnel.
 - Cause 9: The electrical signals sent by the optical module were lost.

Collect alarm, log, and configuration information, and contact technical support personnel.
 - Cause 10: Loss of lock was detected in the receive direction by the optical module.

Collect alarm, log, and configuration information, and contact technical support personnel.
 - Cause 11: Loss of lock was detected in the transmit direction by the optical module.

Collect alarm, log, and configuration information, and contact technical support personnel.
 - Cause 12: The optical module failed to send signals.

Collect alarm, log, and configuration information, and contact technical support personnel.
 - Cause 13: The voltage of the optical module was too high.
 1. Run the display alarm all command to check whether the hwPowerInvalid alarm is generated.
 - If so, go to step 2.
 - If not, go to step 3.
 2. Handle the power alarm and check whether the alarm is cleared.
 - If the alarm is cleared, go to step 8.
 - If the alarm persists, go to step 3.
 3. Check the voltage of the board where the optical module resides and check whether a voltage alarm is generated on the NMS.
 - If so, go to step 4.
 - If not, go to step 5.
 4. Handle the voltage alarm and check whether the alarm is cleared.

- If the alarm is cleared, go to step 8.
 - If the alarm persists, go to step 5.
- 5. Replace the optical module and check whether the alarm is cleared.
 - If the alarm is cleared, go to step 8.
 - If the alarm persists, go to step 6.
- 6. Replace the board where the optical module resides and check whether the alarm is cleared.
 - If the alarm is cleared, go to step 8.
 - If the alarm persists, go to step 7.
- 7. Collect alarm, log, and configuration information, and contact technical support engineers.
- 8. End.
- Cause 14: The voltage of the optical module was too low.
 - 1. Run the display alarm all command to check whether the hwPowerInvalid alarm is generated.
 - If so, go to step 2.
 - If not, go to step 3.
 - 2. Handle the power alarm and check whether the alarm is cleared.
 - If the alarm is cleared, go to step 8.
 - If the alarm persists, go to step 3.
 - 3. Check the voltage of the board where the optical module resides and check whether a voltage alarm is generated on the NMS.
 - If so, go to step 4.
 - If not, go to step 5.
 - 4. Handle the voltage alarm and check whether the alarm is cleared.
 - If the alarm is cleared, go to step 8.
 - If the alarm persists, go to step 5.
 - 5. Replace the optical module and check whether the alarm is cleared.
 - If the alarm is cleared, go to step 8.
 - If the alarm persists, go to step 6.
 - 6. Replace the board where the optical module resides and check whether the alarm is cleared.
 - If the alarm is cleared, go to step 8.
 - If the alarm persists, go to step 7.
 - 7. Collect alarm, log, and configuration information, and contact technical support engineers.
 - 8. End.
- Cause 15: The bias current of the optical module was too high.
 - 1. Run the display alarm all command to check whether the hwPowerInvalid alarm is generated.
 - If so, go to step 2.
 - If not, go to step 3.

2. Handle the power alarm and check whether the alarm is cleared.
 - If the alarm is cleared, go to step 8.
 - If the alarm persists, go to step 3.
 3. Check the current of the board where the optical module resides and check whether a current alarm is generated on the NMS.
 - If so, go to step 4.
 - If not, go to step 5.
 4. Handle the current alarm and check whether the alarm is cleared.
 - If the alarm is cleared, go to step 8.
 - If the alarm persists, go to step 5.
 5. Replace the optical module and check whether the alarm is cleared.
 - If the alarm is cleared, go to step 8.
 - If the alarm persists, go to step 6.
 6. Replace the board where the optical module resides and check whether the alarm is cleared.
 - If the alarm is cleared, go to step 8.
 - If the alarm persists, go to step 7.
 7. Collect alarm, log, and configuration information, and contact technical support engineers.
 8. End.
- Cause 16: The bias current of the optical module was too low.
 1. Run the display alarm all command to check whether the hwPowerInvalid alarm is generated.
 - If so, go to step 2.
 - If not, go to step 3.
 2. Handle the power alarm and check whether the alarm is cleared.
 - If the alarm is cleared, go to step 8.
 - If the alarm persists, go to step 3.
 3. Check the current of the board where the optical module resides and check whether a current alarm is generated on the NMS.
 - If so, go to step 4.
 - If not, go to step 5.
 4. Handle the current alarm and check whether the alarm is cleared.
 - If the alarm is cleared, go to step 8.
 - If the alarm persists, go to step 5.
 5. Replace the optical module and check whether the alarm is cleared.
 - If the alarm is cleared, go to step 8.
 - If the alarm persists, go to step 6.
 6. Replace the board where the optical module resides and check whether the alarm is cleared.
 - If the alarm is cleared, go to step 8.
 - If the alarm persists, go to step 7.

7. Collect alarm, log, and configuration information, and contact technical support engineers.
8. End.
- Cause 17: The temperature of the optical module was too high.
 1. Run the display alarm all command to check whether the hwBoardInvalid alarm is generated.
 - If so, go to step 2.
 - If not, go to step 3.
 2. Handle the alarm and check whether the alarm is cleared.
 - If the alarm is cleared, go to step 8.
 - If the alarm persists, go to step 3.
 3. Check the temperature of the board where the optical module resides and check whether a board temperature alarm is generated on the NMS.
 - If yes, go to step 4.
 - If no, go to step 5.
 4. Handle the board temperature alarm, and then check whether the alarm is cleared.
 - If the alarm is cleared, go to step 8.
 - If the alarm persists, go to step 5.
 5. Replace the optical module and check whether the alarm is cleared.
 - If the alarm is cleared, go to step 8.
 - If the alarm persists, go to step 6.
 6. Replace the board where the optical module resides and check whether the alarm is cleared.
 - If the alarm is cleared, go to step 8.
 - If the alarm persists, go to step 7.
 7. Collect alarm, log, and configuration information, and contact technical support engineers.
 8. End.
- Cause 18: The temperature of the optical module was too low.
 1. Run the display alarm all command to check whether a temperature alarm is generated.
 - If so, go to step 2.
 - If not, go to step 3.
 2. Handle the temperature alarm and check whether the alarm is cleared.
 - If the alarm is cleared, go to step 8.
 - If the alarm persists, go to step 3.
 3. Check the temperature of the board where the optical module resides and check whether a board temperature alarm is generated on the NMS.
 - If so, go to step 4.
 - If not, go to step 5.
 4. Handle the board temperature alarm, and then check whether the alarm is cleared.

- If the alarm is cleared, go to step 8.
 - If the alarm persists, go to step 5.
- 5. Replace the optical module and check whether the alarm is cleared.
 - If the alarm is cleared, go to step 8.
 - If the alarm persists, go to step 6.
- 6. Replace the board where the optical module resides and check whether the alarm is cleared.
 - If the alarm is cleared, go to step 8.
 - If the alarm persists, go to step 7.
- 7. Collect alarm, log, and configuration information, and contact technical support engineers.
- 8. End.
- Cause 19: The power current of the optical module is too high.
 1. Run the display alarm all command to check whether the hwPowerInvalid alarm is generated.
 - If so, go to step 2.
 - If not, go to step 3.
 2. Handle the power alarm and check whether the alarm is cleared.
 - If the alarm is cleared, go to step 8.
 - If the alarm persists, go to step 3.
 3. Check the current of the board where the optical module resides and check whether a current alarm is generated on the NMS.
 - If so, go to step 4.
 - If not, go to step 5.
 4. Handle the current alarm and check whether the alarm is cleared.
 - If the alarm is cleared, go to step 8.
 - If the alarm persists, go to step 5.
 5. Replace the optical module and check whether the alarm is cleared.
 - If the alarm is cleared, go to step 8.
 - If the alarm persists, go to step 6.
 6. Replace the board where the optical module resides and check whether the alarm is cleared.
 - If the alarm is cleared, go to step 8.
 - If the alarm persists, go to step 7.
 7. Collect alarm, log, and configuration information, and contact technical support engineers.

3.5.5.17 ALM-135462923 hwBrdTempFatalAlarm

Description

The board temperature exceeded the fatal alarm threshold.
(EntPhysicalIndex=[EntPhysicalIndex], EntPhysicalName=[EntPhysicalName],
EntityThresholdType=[EntityThresholdType],

```
EntityThresholdCritical=[EntityThresholdCritical],  
EntityThresholdCurrent=[EntityThresholdCurrent],  
EntityTrapFaultID=[EntityTrapFaultID],Reason=[ReasonDsp])
```

A major alarm was generated for the board or subcard temperature.

Attribute

AlarmID	Alarm OID	Alarm Severity	Alarm Type
135462923	1.3.6.1.4.1.2011.5.25 .219.2.10.15	Critical	Environmental alarm

Parameters

Name	Meaning
OID	Indicates the MIB object ID of the alarm.
EntPhysicalIndex	Entity index.
EntPhysicalName	Entity Name
EntityThresholdType	Entity Threshold Type
EntityThresholdCritical	Entity temperature threshold
EntityThresholdCurrent	Current temperature.
EntityTrapFaultID	Fault Code
ReasonDsp	Alarm cause

Impact on the System

- Cause 1: The board temperature was extremely high.
The temperature of the board is too high, which may cause the board to reset.
The temperature of the board is too high, which may cause the board to be powered off.
- Cause 2: The card temperature was extremely high.
The subcard temperature is too high, which may cause the board to reset.

Possible Causes

- Cause 1: The board temperature was extremely high.
- Cause 2: The card temperature was extremely high.

Procedure

- Cause 1: The board temperature was extremely high.
 1. Check whether the air filter of the fan is blocked.
 - If yes, clean the air filter.
 - If not, go to step 2.
 2. Check whether the temperature in the environment is excessively high.
 - If yes, lower the ambient temperature.
 - If not, go to step 3.
 3. Check whether the fan is faulty.
 - If yes, rectify the fan fault.
 - If no, go to Step 4.
 4. Check whether filler panels are installed in vacant slots.
 - If yes, go to step 5.
 - If not, insert a filler panel.
 5. Collect alarm, log, and configuration information and contact technical support personnel.
- Cause 2: The card temperature was extremely high.
 1. Check whether the air filter of the fan is blocked.
 - If yes, clean the air filter.
 - If not, go to step 2.
 2. Check whether the temperature in the environment is excessively high.
 - If yes, lower the ambient temperature.
 - If not, go to step 3.
 3. Check whether the fan is faulty.
 - If yes, rectify the fan fault.
 - If no, go to Step 4.
 4. Check whether a filler panel is installed in the vacant slot.
 - If yes, go to step 5.
 - If not, insert a filler panel.
 5. Collect alarm, log, and configuration information and contact technical support personnel.

3.5.5.18 ALM-15794223 hwEthHalfDuplex

Description

Eth half duplex.

(InterfaceIndex=[hwPhysicalPortIfIndex],InterfaceName=[hwPhysicalPortName])

The interface is negotiated to work in half-duplex mode. As a result, a large number of packets are lost.

Attribute

AlarmID	Alarm OID	Alarm Severity	Alarm Type
15794223	1.3.6.1.4.1.2011.5.25 .157.2.207	Warning	Processing error alarm

Parameters

Name	Meaning
hwPhysicalPortIfIndex	Physical interface index.
hwPhysicalPortName	Physical interface name.

Impact on the System

In half-duplex mode, if bidirectional traffic is transmitted, packet loss may occur due to conflicts.

Possible Causes

Port configurations are different between the two sides (one port is set to speed force, and the other port is set to negotiation). As a result, the ports negotiate to half-duplex, and packet loss occurs, triggering a half-duplex alarm.

Procedure

1. Check whether the rates of the interconnected interfaces at both ends are the same. If not, change them to be the same.
2. Check whether the cable connection is correct. If yes, rectify the fault. Check whether the alarm is cleared.
 - If the alarm is cleared, go to Step 4.
 - If the alarm persists, go to Step 3.
3. Collect alarm, log, and configuration information, and contact Huawei technical support personnel.
4. End.

3.5.5.19 ALM-135602186 RESTORE_CONFIGURATION_FAIL

Description

Failed to restore system configurations. (Result=[Result])

The system configurations failed to be restored.

Attribute

AlarmID	Alarm OID	Alarm Severity	Alarm Type
135602186	1.3.6.1.4.1.2011.5.25 .157.2.207	Major	Processing error alarm

Parameters

Name	Meaning
Result	Configuration restoration result

Impact on the System

If the default configuration file is available, it will be started using the default configuration file, and if neither is available, it will cause an empty configuration to start.

Possible Causes

The configuration file consistency verification failed or failed for an unknown reason.

Procedure

Use or re create the configuration file, and set it to restart again after the configuration file is started next time.