



Brocade[®] Fabric OS[®] Message Reference Manual, 9.2.x

**Technical Reference Manual
June 30, 2023**

Table of Contents

Introduction.....	77
Supported Hardware and Software.....	77
Brocade Gen 7 (64G) Fixed-Port Switches.....	77
Brocade Gen 7 (64G) Directors.....	77
Brocade Gen 6 (32G) Fixed-Port Switches.....	77
Brocade Gen 6 (32G) Directors.....	77
Contacting Technical Support for Your Brocade® Product.....	77
Document Feedback.....	78
Overview of System Messages.....	79
System Message Types.....	79
Log Messages.....	79
Audit Messages.....	79
Audit Log Enhancements.....	80
Audit Messages Related to SSH.....	82
Audit Messages Related to TLS.....	83
Audit Messages Related to Certificate Validation.....	84
Audit Messages Related to When Unsecure Protocols Are Allowed or Secure Protocols Are Disabled.....	84
FFDC Messages.....	85
Message Severity Levels.....	85
System Error Message Logging.....	86
Configuring Syslog Message Destinations.....	86
System Logging Daemon.....	86
Configuring a Syslog Server.....	87
System Console.....	87
Setting the System Console Severity Level.....	87
SNMP Trap Recipient.....	88
Configuring the SNMPv1 Trap Recipient.....	88
Configuring the SNMPv3 Trap Recipient.....	89
SNMP Inform Recipient.....	91
Configuring the SNMPv3 Inform Recipient.....	91
Port Logs.....	92
Changing the swEventTrap Severity Level.....	93
Commands for Displaying and Configuring System Message Logs.....	94
Displaying Message Content on the Switch.....	95
Configuring System Messages and Attributes.....	96
Configuring Event Auditing.....	96

Disabling a RASLog Message or Module.....	97
Enabling a RASLog Message or Module.....	97
Setting the Severity Level of a RASLog Message.....	97
Enabling Quiet Time for a Specified Message Type.....	98
Disabling Quiet Time for a Specified Message Type.....	98
Displaying System Message Logs and Attributes.....	98
Displaying RASLog Messages.....	98
Displaying RASLog Messages One Message at a Time.....	99
Displaying Audit Messages.....	99
Displaying FFDC Messages.....	99
Displaying the Status of System Messages.....	100
Displaying the Severity Level of RASLog Messages.....	100
Displaying the Configured Quiet Time.....	100
Displaying RASLog Messages by Severity Level.....	101
Displaying RASLog Messages by Message ID.....	101
Displaying Messages on a Slot.....	101
Viewing RASLog Messages from Web Tools.....	102
Clearing System Message Logs.....	102
Clearing the System Message Log.....	102
Clearing the Audit Message Log.....	102
Reading System Messages.....	102
Reading a RAS System Message.....	102
Reading an Audit Message.....	104
Responding to System Messages.....	105
Looking Up a System Message.....	105
Gathering Information about the Problem.....	105
Troubleshooting Files for Support Personnel.....	106
Panic Dump and Core Dump Files.....	106
Trace Dumps.....	106
supportSave Command.....	107
Troubleshooting FFDC.....	107
System Module Descriptions.....	107
Fabric OS System Messages.....	115
AG Messages.....	115
AG-1001.....	115
AG-1002.....	115
AG-1003.....	116
AG-1004.....	116
AG-1005.....	117
AG-1006.....	117

AG-1007.....	118
AG-1008.....	118
AG-1009.....	118
AG-1010.....	119
AG-1011.....	119
AG-1012.....	120
AG-1013.....	120
AG-1014.....	121
AG-1015.....	121
AG-1016.....	122
AG-1017.....	122
AG-1018.....	122
AG-1019.....	123
AG-1020.....	123
AG-1021.....	124
AG-1022.....	124
AG-1023.....	125
AG-1024.....	125
AG-1025.....	125
AG-1026.....	126
AG-1027.....	126
AG-1028.....	127
AG-1029.....	127
AG-1030.....	128
AG-1031.....	128
AG-1032.....	128
AG-1033.....	129
AG-1034.....	129
AG-1035.....	130
AG-1036.....	130
AG-1037.....	131
AG-1038.....	131
AG-1039.....	132
AG-1040.....	132
AG-1041.....	132
AG-1042.....	133
AG-1043.....	133
AG-1044.....	134
AG-1045.....	134
AG-1046.....	135

AG-1047.....	135
AG-1048.....	136
AG-1049.....	136
AG-1050.....	137
AG-1051.....	137
AG-1052.....	137
AG-1053.....	138
AG-1054.....	138
AG-1055.....	139
AG-1056.....	139
AG-1057.....	139
AG-1058.....	140
AG-1059.....	140
AG-1060.....	141
AG-1061.....	141
AG-1062.....	141
AG-1063.....	142
AG-1064.....	142
AG-1065.....	143
AG-1066.....	143
AG-1067.....	143
AG-1068.....	144
AG-1069.....	144
AG-1070.....	145
AG-1071.....	145
AG-1072.....	145
AG-1073.....	146
AG-1074.....	146
AG-1075.....	147
AG-1076.....	147
AG-1077.....	147
AG-1078.....	148
AG-1079.....	148
AG-1080.....	149
AG-1081.....	149
AG-1082.....	149
AG-1083.....	150
AG-1084.....	150
AG-1085.....	151
AG-1086.....	151

AG-1087.....	151
AG-1088.....	152
AG-1089.....	152
AG-1090.....	153
AG-1091.....	153
AG-1092.....	154
AG-1093.....	154
AG-1094.....	154
AL Messages.....	155
AL-1003.....	155
AL-1004.....	155
AL-1005.....	156
AL-1006.....	156
AN Messages.....	156
AN-1001.....	156
AN-1002.....	157
AN-1010.....	157
AN-1011.....	158
AN-1012.....	158
AN-1013.....	159
AN-1014.....	159
ASVR Messages.....	160
ASVR-1001.....	160
AUTH Messages.....	160
AUTH-1001.....	160
AUTH-1002.....	160
AUTH-1003.....	161
AUTH-1004.....	161
AUTH-1005.....	162
AUTH-1006.....	162
AUTH-1007.....	163
AUTH-1008.....	163
AUTH-1010.....	164
AUTH-1011.....	164
AUTH-1012.....	165
AUTH-1013.....	165
AUTH-1014.....	165
AUTH-1016.....	166
AUTH-1017.....	166
AUTH-1018.....	167

AUTH-1020.....	167
AUTH-1022.....	168
AUTH-1023.....	168
AUTH-1025.....	169
AUTH-1026.....	170
AUTH-1027.....	170
AUTH-1028.....	171
AUTH-1029.....	171
AUTH-1030.....	172
AUTH-1031.....	172
AUTH-1032.....	173
AUTH-1033.....	173
AUTH-1034.....	174
AUTH-1035.....	174
AUTH-1036.....	175
AUTH-1037.....	175
AUTH-1038.....	176
AUTH-1039.....	176
AUTH-1040.....	177
AUTH-1041.....	177
AUTH-1042.....	178
AUTH-1043.....	178
AUTH-1044.....	179
AUTH-1045.....	179
AUTH-1046.....	180
AUTH-1047.....	180
AUTH-1048.....	181
AUTH-1049.....	181
AUTH-1050.....	182
AUTH-1051.....	182
AUTH-3001.....	183
AUTH-3002.....	183
AUTH-3003.....	184
AUTH-3004.....	184
AUTH-3005.....	185
AUTH-3006.....	185
AUTH-3007.....	186
AUTH-3008.....	187
AUTH-3009.....	187
AUTH-3010.....	188

BCM Messages.....	188
BCM-1000.....	188
BCM-1001.....	189
BCM-1002.....	189
BCM-1003.....	190
BCM-1004.....	190
BCM-1005.....	190
BCM-1006.....	191
BCMG Messages.....	191
BCMG-1000.....	191
BCMG-1001.....	192
BCMG-1002.....	192
BCMG-1003.....	193
BCMG-1004.....	193
BCMG-1005.....	193
BL Messages.....	194
BL-1000.....	194
BL-1001.....	194
BL-1002.....	195
BL-1003.....	195
BL-1004.....	196
BL-1006.....	196
BL-1007.....	197
BL-1008.....	197
BL-1009.....	198
BL-1010.....	198
BL-1011.....	199
BL-1012.....	199
BL-1013.....	200
BL-1014.....	200
BL-1015.....	201
BL-1016.....	202
BL-1017.....	202
BL-1018.....	202
BL-1019.....	203
BL-1020.....	203
BL-1021.....	204
BL-1022.....	204
BL-1023.....	204
BL-1024.....	205

BL-1025.....	205
BL-1026.....	206
BL-1027.....	206
BL-1028.....	206
BL-1029.....	207
BL-1030.....	207
BL-1031.....	208
BL-1032.....	208
BL-1033.....	209
BL-1034.....	209
BL-1035.....	209
BL-1036.....	210
BL-1037.....	210
BL-1038.....	211
BL-1039.....	211
BL-1040.....	212
BL-1041.....	212
BL-1045.....	213
BL-1046.....	213
BL-1047.....	213
BL-1048.....	214
BL-1049.....	214
BL-1050.....	215
BL-1052.....	215
BL-1053.....	215
BL-1054.....	216
BL-1055.....	216
BL-1056.....	217
BL-1057.....	217
BL-1058.....	218
BL-1061.....	218
BL-1062.....	218
BL-1063.....	219
BL-1064.....	219
BL-1065.....	219
BL-1066.....	220
BL-1080.....	220
BL-1081.....	221
BL-1082.....	221
BL-1083.....	222

BL-1084.....	222
BL-1085.....	222
BL-1086.....	223
BL-1087.....	223
BLS Messages.....	224
BLS-1000.....	224
BLS-1001.....	224
BLS-1002.....	225
BLS-1003.....	225
BLS-1004.....	225
BLS-1005.....	226
BM Messages.....	226
BM-1001.....	226
BM-1002.....	227
BM-1003.....	227
BM-1004.....	228
BM-1005.....	228
BM-1006.....	228
BM-1007.....	229
BM-1008.....	229
BM-1009.....	230
BM-1010.....	230
BM-1053.....	231
BM-1054.....	231
BM-1055.....	232
BM-1056.....	232
BM-1058.....	232
C4 Messages.....	233
C4-1001.....	233
C4-1002.....	233
C4-1004.....	234
C4-1006.....	234
C4-1007.....	235
C4-1008.....	235
C4-1009.....	235
C4-1010.....	236
C4-1011.....	236
C4-1012.....	237
C4-1013.....	237
C4-1014.....	238

C4-1015.....	238
C4-1016.....	239
C4-1017.....	239
C4-1018.....	239
C4-1019.....	240
C4-1020.....	240
C4-1023.....	241
C4-1028.....	241
C4-1030.....	242
C4-1031.....	242
C4-1032.....	242
C4-1033.....	243
C4-1034.....	243
C4-1035.....	244
C4-1036.....	244
C4-1037.....	244
C4-1038.....	245
C4-1039.....	245
C4-1040.....	246
C4-1041.....	246
C4-1042.....	246
C4-1043.....	247
C4-1044.....	247
C4-1045.....	248
C4-1046.....	248
C4-1047.....	249
C4-1048.....	249
C4-1049.....	250
C4-1050.....	250
C4-1051.....	251
C4-1052.....	251
C4-1054.....	252
C4-1055.....	252
C4-1056.....	252
C5 Messages.....	253
C5-1001.....	253
C5-1002.....	253
C5-1004.....	254
C5-1006.....	254
C5-1007.....	255

C5-1008.....	255
C5-1009.....	255
C5-1010.....	256
C5-1011.....	256
C5-1012.....	257
C5-1013.....	257
C5-1014.....	258
C5-1015.....	258
C5-1016.....	259
C5-1017.....	259
C5-1018.....	259
C5-1019.....	260
C5-1020.....	260
C5-1023.....	261
C5-1028.....	261
C5-1030.....	262
C5-1031.....	262
C5-1032.....	262
C5-1033.....	263
C5-1034.....	263
C5-1035.....	264
C5-1036.....	264
C5-1037.....	264
C5-1038.....	265
C5-1039.....	265
C5-1040.....	266
C5-1041.....	266
C5-1042.....	266
C5-1043.....	267
C5-1044.....	267
C5-1045.....	268
C5-1046.....	268
C5-1048.....	269
C5-1049.....	269
C5-1050.....	270
C5-1051.....	270
C5-1052.....	271
C5-1053.....	271
C5-1054.....	272
C5-1055.....	272

C5-1056.....	272
C5-1057.....	273
CAL Messages.....	273
CAL-1001.....	273
CDR Messages.....	274
CDR-1001.....	274
CDR-1002.....	274
CDR-1003.....	275
CDR-1004.....	275
CDR-1005.....	276
CDR-1006.....	276
CDR-1007.....	276
CDR-1008.....	277
CDR-1009.....	277
CDR-1010.....	278
CDR-1011.....	278
CDR-1012.....	279
CDR-1014.....	279
CDR-1015.....	279
CDR-1016.....	280
CDR-1017.....	280
CDR-1018.....	281
CDR-1019.....	281
CDR-1022.....	282
CDR-1028.....	282
CFG Messages.....	282
CFG-1001.....	283
CFG-1002.....	283
CH Messages.....	283
CH-1001.....	284
CH-1002.....	284
CHS Messages.....	284
CHS-1002.....	284
CHS-1003.....	285
CHS-1004.....	285
CHS-1005.....	286
CHS-1006.....	286
CHS-1007.....	287
CHS-1008.....	287
CNM Messages.....	287

CNM-1001.....	287
CNM-1002.....	288
CNM-1003.....	288
CNM-1004.....	289
CNM-1005.....	289
CNM-1006.....	289
CNM-1007.....	290
CNM-1008.....	290
CNM-1009.....	290
CNM-1010.....	291
CNM-1011.....	291
CNM-1012.....	291
CNM-1013.....	292
CNM-1014.....	292
CNM-1015.....	292
CNM-1016.....	293
CNM-1017.....	293
CNM-1018.....	293
CNM-1019.....	294
CNM-1020.....	294
CNM-1021.....	295
CNM-1022.....	295
CNM-1023.....	295
CNM-1024.....	296
CNM-1025.....	296
CNM-1026.....	296
CNM-1027.....	297
CNM-1028.....	297
CNM-1029.....	297
CNM-1030.....	298
CNM-1031.....	298
CNM-1032.....	298
CNM-1033.....	299
CNM-1034.....	299
CNM-1035.....	299
CNM-1036.....	300
CNM-1037.....	300
CNM-1038.....	300
CNM-1039.....	301
CNM-1040.....	301

CNM-1041.....	301
CNM-1042.....	302
CNM-1043.....	302
CNM-1044.....	302
CNM-1045.....	303
CNM-1046.....	303
CNM-1047.....	303
CNM-1048.....	304
CNM-1049.....	304
CNM-1050.....	304
CNM-1051.....	305
CNM-1052.....	305
CNM-1053.....	306
CNM-1054.....	306
CNM-1055.....	306
CNM-1056.....	307
CNM-1057.....	307
CNM-1058.....	307
CNM-1059.....	308
CNM-1060.....	308
CNM-1061.....	308
CNM-1062.....	309
CNM-3001.....	309
CNM-3002.....	309
CNM-3003.....	310
CNM-3004.....	310
CNM-3005.....	311
CNM-3006.....	311
CNM-3007.....	311
CNM-3008.....	312
CNM-3009.....	312
CNM-3010.....	313
CNM-3011.....	313
CNM-3012.....	313
CNMC Messages.....	314
CNMC-1001.....	314
CNMC-1002.....	314
CNMC-1003.....	315
CONF Messages.....	315
CONF-1000.....	315

CONF-1001.....	316
CONF-1020.....	316
CONF-1021.....	317
CONF-1022.....	317
CONF-1023.....	317
CONF-1024.....	318
CONF-1030.....	318
CONF-1031.....	319
CONF-1032.....	319
CONF-1033.....	320
CONF-1040.....	320
CONF-1041.....	320
CONF-1042.....	321
CONF-1043.....	321
CONF-1044.....	322
CONF-1045.....	322
CONF-1046.....	322
CONF-1047.....	323
CONF-1048.....	323
CONF-1049.....	324
CONF-1050.....	324
CONF-1051.....	324
CONF-1052.....	325
CONF-1053.....	325
CONF-1054.....	326
CONF-1055.....	326
DIAG Messages.....	326
DIAG-1000.....	326
ECC Messages.....	327
ECC-1000.....	327
ECC-1001.....	327
EM Messages.....	328
EM-1001.....	328
EM-1002.....	328
EM-1003.....	329
EM-1004.....	329
EM-1005.....	330
EM-1006.....	330
EM-1008.....	331
EM-1009.....	331

EM-1010.....	332
EM-1011.....	332
EM-1012.....	333
EM-1013.....	333
EM-1014.....	334
EM-1015.....	334
EM-1016.....	334
EM-1017.....	335
EM-1018.....	335
EM-1019.....	336
EM-1020.....	336
EM-1028.....	337
EM-1029.....	337
EM-1031.....	338
EM-1033.....	338
EM-1034.....	339
EM-1035.....	339
EM-1036.....	340
EM-1037.....	340
EM-1042.....	341
EM-1043.....	341
EM-1044.....	342
EM-1045.....	342
EM-1046.....	343
EM-1047.....	343
EM-1048.....	344
EM-1049.....	344
EM-1050.....	344
EM-1051.....	345
EM-1057.....	345
EM-1058.....	346
EM-1059.....	346
EM-1060.....	347
EM-1061.....	347
EM-1062.....	348
EM-1063.....	348
EM-1064.....	348
EM-1065.....	349
EM-1066.....	349
EM-1067.....	350

EM-1068.....	350
EM-1069.....	351
EM-1070.....	351
EM-1071.....	351
EM-1072.....	352
EM-1073.....	352
EM-1074.....	353
EM-1075.....	353
EM-1076.....	354
EM-1100.....	354
EM-1101.....	354
EM-1134.....	355
EM-1220.....	355
EM-1221.....	356
EM-1222.....	356
EM-1223.....	357
EM-1224.....	357
EM-1225.....	358
EM-1226.....	358
EM-1227.....	358
EM-1228.....	359
EM-1229.....	359
EM-1230.....	360
EM-1235.....	360
EM-1240.....	361
EM-1241.....	361
EM-2003.....	361
EM-2004.....	362
ERCP Messages.....	362
ERCP-1000.....	362
ERCP-1001.....	363
ERCP-1002.....	363
ESM Messages.....	364
ESM-1000.....	364
ESM-1001.....	364
ESM-1002.....	364
ESM-1003.....	365
ESM-1004.....	365
ESM-1005.....	365
ESM-1010.....	366

ESM-1011.....	366
ESM-1012.....	367
ESM-1013.....	367
ESM-1100.....	367
ESM-1101.....	368
ESM-1102.....	368
ESM-1103.....	369
ESM-1104.....	369
ESM-1105.....	370
ESM-1106.....	370
ESM-2000.....	371
ESM-2001.....	371
ESM-2002.....	371
ESM-2010.....	372
ESM-2011.....	372
ESM-2012.....	373
ESM-2100.....	373
ESM-2101.....	373
ESM-2102.....	374
ESM-2103.....	374
ESM-2104.....	375
ESM-2105.....	375
ESM-2106.....	375
ESM-2200.....	376
ESM-2201.....	376
ESM-2202.....	377
ESM-2203.....	377
ESM-2300.....	377
ESM-2301.....	378
ESM-2302.....	378
ESM-2303.....	379
ESM-2310.....	379
ESM-2311.....	379
ESM-2312.....	380
ESM-2313.....	380
ESM-2314.....	381
ESM-2315.....	381
ESM-2316.....	382
ESM-2317.....	382
ESM-2318.....	382

ESM-2319.....	383
ESM-2320.....	383
ESM-2321.....	384
ESM-2322.....	384
ESM-2323.....	385
ESM-2324.....	385
ESM-2325.....	385
ESM-2326.....	386
ESM-2327.....	386
ESM-2328.....	387
ESM-2329.....	387
ESM-2400.....	388
ESM-2700.....	388
ESM-2701.....	388
ESM-2702.....	389
ESM-2703.....	389
ESM-2801.....	390
ESM-2802.....	390
ESM-2803.....	390
ESM-3000.....	391
ESM-3001.....	391
ESM-3002.....	391
ESM-3003.....	392
ESM-3004.....	392
ESM-3005.....	392
ESM-3006.....	393
ESM-3007.....	393
ESM-3008.....	394
ESM-3100.....	394
ESM-3101.....	394
ESM-3102.....	395
ESM-3103.....	395
ESM-3104.....	395
ESS Messages.....	396
ESS-1001.....	396
ESS-1002.....	396
ESS-1003.....	397
ESS-1004.....	397
ESS-1005.....	397
ESS-1008.....	398

ESS-1009.....	398
ESS-1010.....	399
ESS-1011.....	399
ESS-1012.....	400
ESS-2001.....	400
ESS-2002.....	401
ESW Messages.....	401
ESW-1001.....	401
ESW-1002.....	401
ESW-1003.....	402
ESW-1004.....	402
ESW-1005.....	403
ESW-1006.....	403
ESW-1007.....	404
ESW-1008.....	404
EVMD Messages.....	404
EVMD-1001.....	405
EXDP Messages.....	405
EXDP-1005.....	405
EXDP-1006.....	406
EXDP-1007.....	406
EXDP-1008.....	406
FABR Messages.....	407
FABR-1001.....	407
FABR-1002.....	407
FABR-1003.....	408
FABR-1004.....	408
FABR-1005.....	409
FABR-1006.....	409
FABR-1007.....	410
FABR-1008.....	410
FABR-1009.....	411
FABR-1010.....	411
FABR-1011.....	412
FABR-1012.....	412
FABR-1013.....	413
FABR-1014.....	413
FABR-1015.....	414
FABR-1016.....	414
FABR-1017.....	415

FABR-1018.....	415
FABR-1019.....	415
FABR-1020.....	416
FABR-1021.....	416
FABR-1022.....	417
FABR-1023.....	417
FABR-1024.....	418
FABR-1029.....	418
FABR-1030.....	419
FABR-1031.....	419
FABR-1032.....	420
FABR-1034.....	420
FABR-1035.....	421
FABR-1036.....	421
FABR-1037.....	421
FABR-1038.....	422
FABR-1039.....	422
FABR-1040.....	423
FABR-1041.....	423
FABR-1043.....	424
FABR-1044.....	424
FABR-1045.....	424
FABR-1046.....	425
FABR-1047.....	425
FABR-1048.....	426
FABR-1049.....	426
FABR-1050.....	427
FABR-1051.....	427
FABR-1052.....	428
FABR-1053.....	428
FABR-1054.....	428
FABR-1055.....	429
FABR-1056.....	429
FABR-1057.....	430
FABR-1058.....	430
FABR-1059.....	430
FABR-1060.....	431
FABR-1061.....	431
FABR-1062.....	432
FABR-1063.....	432

FABR-1064.....	433
FABR-1065.....	433
FABR-1066.....	434
FABR-1067.....	434
FABR-3000.....	435
FABS Messages.....	435
FABS-1001.....	435
FABS-1002.....	436
FABS-1004.....	436
FABS-1005.....	436
FABS-1006.....	437
FABS-1007.....	438
FABS-1008.....	438
FABS-1009.....	438
FABS-1010.....	439
FABS-1011.....	439
FABS-1013.....	440
FABS-1014.....	440
FABS-1015.....	441
FBC Messages.....	441
FBC-1001.....	441
FCLG Messages.....	442
FCLG-1001.....	442
FCMC Messages.....	442
FCMC-1001.....	442
FCOE Messages.....	443
FCOE-1001.....	443
FCOE-1002.....	443
FCOE-1003.....	444
FCOE-1004.....	444
FCOE-1005.....	445
FCOE-1006.....	445
FCOE-1007.....	445
FCOE-1008.....	446
FCOE-1009.....	446
FCOE-1010.....	447
FCOE-1011.....	447
FCOE-1019.....	447
FCOE-1022.....	448
FCOE-1023.....	448

FCOE-1024.....	449
FCOE-1029.....	449
FCOE-1030.....	450
FCOE-1032.....	450
FCOE-1033.....	450
FCOE-1034.....	451
FCOE-1037.....	451
FCOE-1038.....	452
FCOE-1039.....	452
FCOE-1040.....	452
FCOE-1041.....	453
FCOE-1042.....	453
FCOE-1043.....	453
FCOE-1044.....	454
FCPD Messages.....	454
FCPD-1001.....	454
FCPD-1002.....	455
FCPD-1003.....	455
FCPH Messages.....	456
FCPH-1001.....	456
FCPH-1002.....	456
FCPH-1003.....	457
FCPH-1004.....	457
FCPH-1005.....	457
FCPH-1006.....	458
FCPH-1007.....	458
FCPH-1008.....	459
FCPH-1009.....	459
FCPH-1010.....	459
FCPH-1011.....	460
FCPH-1012.....	460
FCPH-1013.....	461
FCPH-1014.....	461
FCR Messages.....	461
FCR-1001.....	462
FCR-1002.....	462
FCR-1003.....	462
FCR-1004.....	463
FCR-1005.....	463
FCR-1006.....	463

FCR-1007.....	464
FCR-1008.....	464
FCR-1009.....	464
FCR-1010.....	465
FCR-1011.....	465
FCR-1012.....	465
FCR-1013.....	466
FCR-1015.....	466
FCR-1016.....	466
FCR-1018.....	467
FCR-1019.....	467
FCR-1020.....	468
FCR-1021.....	468
FCR-1022.....	469
FCR-1023.....	469
FCR-1024.....	470
FCR-1025.....	470
FCR-1026.....	470
FCR-1027.....	471
FCR-1028.....	471
FCR-1029.....	472
FCR-1030.....	472
FCR-1031.....	473
FCR-1032.....	473
FCR-1033.....	473
FCR-1034.....	474
FCR-1035.....	474
FCR-1036.....	474
FCR-1037.....	475
FCR-1038.....	475
FCR-1039.....	476
FCR-1040.....	476
FCR-1041.....	476
FCR-1042.....	477
FCR-1043.....	477
FCR-1048.....	477
FCR-1049.....	478
FCR-1053.....	478
FCR-1054.....	479
FCR-1055.....	479

FCR-1056.....	480
FCR-1057.....	480
FCR-1058.....	481
FCR-1059.....	481
FCR-1060.....	482
FCR-1061.....	482
FCR-1062.....	482
FCR-1063.....	483
FCR-1064.....	483
FCR-1065.....	484
FCR-1066.....	484
FCR-1067.....	485
FCR-1068.....	485
FCR-1069.....	486
FCR-1070.....	486
FCR-1071.....	486
FCR-1072.....	487
FCR-1073.....	487
FCR-1074.....	488
FCR-1075.....	488
FCR-1076.....	489
FCR-1077.....	489
FCR-1078.....	489
FCR-1079.....	490
FCR-1080.....	490
FCR-1081.....	491
FCR-1082.....	491
FCR-1083.....	491
FCR-1084.....	492
FCR-1085.....	492
FCR-1086.....	493
FCR-1087.....	493
FCR-1088.....	494
FCR-1089.....	494
FCR-1091.....	494
FCR-1092.....	495
FCR-1093.....	495
FCR-1094.....	496
FCR-1095.....	496
FCR-1096.....	497

FCR-1097.....	497
FCR-1098.....	498
FCR-1099.....	498
FCR-1100.....	499
FCR-1101.....	499
FCR-1102.....	499
FCR-1103.....	500
FCR-1104.....	500
FCR-1105.....	501
FCR-1106.....	501
FCR-1107.....	502
FCR-1108.....	502
FCR-1109.....	502
FCR-1110.....	503
FCR-1111.....	503
FCR-1112.....	504
FCR-1113.....	504
FCR-1114.....	505
FCR-1115.....	505
FCR-1116.....	505
FCR-1117.....	506
FCR-1118.....	506
FCR-1119.....	507
FCR-1120.....	507
FCR-1121.....	507
FCR-1122.....	508
FCR-1123.....	508
FCR-1124.....	509
FCR-1125.....	509
FCR-1126.....	509
FICN Messages.....	510
FICN-1007.....	510
FICN-1008.....	510
FICN-1010.....	511
FICN-1011.....	511
FICN-1012.....	512
FICN-1013.....	512
FICN-1014.....	513
FICN-1015.....	513
FICN-1016.....	514

FICN-1017.....	514
FICN-1019.....	514
FICN-1020.....	515
FICN-1021.....	515
FICN-1022.....	516
FICN-1023.....	516
FICN-1024.....	517
FICN-1025.....	517
FICN-1026.....	518
FICN-1027.....	518
FICN-1028.....	518
FICN-1029.....	519
FICN-1030.....	519
FICN-1032.....	520
FICN-1033.....	520
FICN-1034.....	521
FICN-1035.....	521
FICN-1036.....	522
FICN-1037.....	522
FICN-1040.....	522
FICN-1041.....	523
FICN-1042.....	523
FICN-1043.....	524
FICN-1044.....	524
FICN-1045.....	525
FICN-1046.....	525
FICN-1047.....	526
FICN-1048.....	526
FICN-1049.....	527
FICN-1050.....	527
FICN-1051.....	528
FICN-1052.....	528
FICN-1053.....	528
FICN-1054.....	529
FICN-1055.....	529
FICN-1056.....	530
FICN-1057.....	530
FICN-1059.....	531
FICN-1062.....	531
FICN-1063.....	532

FICN-1067.....	532
FICN-1068.....	532
FICN-1070.....	533
FICN-1071.....	533
FICN-1072.....	534
FICN-1073.....	534
FICN-1074.....	534
FICN-1075.....	535
FICN-1076.....	535
FICN-1077.....	536
FICN-1078.....	536
FICN-1079.....	537
FICN-1080.....	537
FICN-1081.....	537
FICN-1087.....	538
FICN-1088.....	538
FICN-1089.....	539
FICN-1090.....	539
FICN-1091.....	540
FICN-1092.....	540
FICN-1093.....	541
FICN-1094.....	541
FICN-1095.....	542
FICN-1096.....	542
FICN-1097.....	543
FICN-1098.....	543
FICN-1099.....	544
FICN-1100.....	544
FICN-1101.....	545
FICN-1102.....	545
FICN-1103.....	546
FICN-1104.....	546
FICN-1105.....	546
FICN-1106.....	547
FICN-1107.....	547
FICN-1108.....	548
FICN-1109.....	548
FICN-1110.....	549
FICN-1111.....	549
FICN-1112.....	550

FICN-1113.....	550
FICN-1114.....	551
FICN-1115.....	551
FICN-1116.....	552
FICN-1117.....	552
FICN-1118.....	553
FICN-1119.....	553
FICN-1120.....	554
FICN-1121.....	554
FICN-1122.....	555
FICN-1123.....	555
FICN-2064.....	555
FICN-2065.....	556
FICN-2066.....	556
FICN-2082.....	557
FICN-2087.....	557
FICU Messages.....	558
FICU-1001.....	558
FICU-1002.....	558
FICU-1003.....	559
FICU-1004.....	559
FICU-1005.....	560
FICU-1006.....	560
FICU-1007.....	561
FICU-1008.....	561
FICU-1009.....	561
FICU-1010.....	562
FICU-1011.....	562
FICU-1012.....	563
FICU-1013.....	563
FICU-1017.....	563
FICU-1018.....	564
FICU-1019.....	564
FICU-1020.....	565
FICU-1021.....	565
FICU-1022.....	566
FICU-1025.....	566
FICU-1026.....	566
FICU-1030.....	567
FICU-1031.....	567

FICU-1032.....	567
FICU-1033.....	568
FICU-1035.....	568
FICU-1036.....	569
FICU-1037.....	569
FKLB Messages.....	569
FKLB-1001.....	570
FLOD Messages.....	570
FLOD-1001.....	570
FLOD-1003.....	570
FLOD-1004.....	571
FLOD-1005.....	571
FLOD-1006.....	572
FLOD-1007.....	572
FSPF Messages.....	573
FSPF-1001.....	573
FSPF-1002.....	573
FSPF-1003.....	573
FSPF-1005.....	574
FSPF-1006.....	574
FSPF-1007.....	575
FSPF-1008.....	575
FSPF-1009.....	576
FSPF-1010.....	576
FSPF-1011.....	576
FSPF-1012.....	577
FSPF-1013.....	577
FSPF-1014.....	578
FSPF-1015.....	578
FSPF-1016.....	578
FSPF-1017.....	579
FSPF-1018.....	579
FSPF-1019.....	580
FSPF-1020.....	580
FSS Messages.....	580
FSS-1001.....	580
FSS-1002.....	581
FSS-1003.....	581
FSS-1004.....	582
FSS-1005.....	582

FSS-1006.....	583
FSS-1007.....	583
FSS-1008.....	584
FSS-1009.....	584
FSS-1010.....	585
FSS-1011.....	585
FSSM Messages.....	585
FSSM-1002.....	585
FSSM-1003.....	586
FSSM-1004.....	586
FSSM-1005.....	587
FTC Messages.....	587
FTC-1001.....	587
FTC-1002.....	588
FV Messages.....	588
FV-1001.....	588
FV-1002.....	589
FV-1003.....	589
FV-1004.....	589
FV-1007.....	590
FV-1008.....	590
FV-1009.....	591
FV-1010.....	591
FV-1011.....	591
FV-1012.....	592
FV-3000.....	592
FV-3001.....	592
FV-3002.....	593
FV-3003.....	593
FV-3004.....	594
FV-3005.....	594
FV-3006.....	594
FV-3007.....	595
FV-3008.....	595
FV-3009.....	596
FV-3010.....	596
FV-3011.....	597
FV-3012.....	597
FV-3013.....	597
FV-3014.....	598

FV-3015.....	598
FV-3016.....	599
FV-3017.....	599
FV-3018.....	599
FV-3019.....	600
FV-3020.....	600
FV-3021.....	600
FV-3022.....	601
FV-3023.....	601
FV-3024.....	601
FV-3025.....	602
FV-3026.....	602
FV-3027.....	602
FVS Messages.....	603
FVS-1001.....	603
GE5 Messages.....	603
GE5-1001.....	603
GE5-1002.....	604
GE5-1004.....	604
GE5-1006.....	605
GE5-1007.....	605
GE5-1008.....	605
GE5-1009.....	606
GE5-1010.....	606
GE5-1011.....	607
GE5-1012.....	607
GE5-1013.....	608
GE5-1014.....	608
GE5-1015.....	609
GE5-1016.....	609
GE5-1017.....	609
GE5-1018.....	610
GE5-1019.....	610
GE5-1020.....	611
GE5-1023.....	611
GE5-1028.....	612
GE5-1030.....	612
GE5-1031.....	612
GE5-1032.....	613
GE5-1033.....	613

GE5-1034.....	614
GE5-1035.....	614
GE5-1036.....	615
GE5-1037.....	615
GE5-1038.....	615
GE5-1039.....	616
GE5-1040.....	616
GE5-1041.....	617
GE5-1042.....	617
GE5-1043.....	617
GE5-1044.....	618
GE5-1045.....	618
GE5-1046.....	619
GE5-1048.....	619
GE5-1049.....	620
GE5-1050.....	620
GE5-1051.....	621
GE5-1052.....	621
GE5-1053.....	622
GE5-1054.....	622
GE5-1055.....	622
GE5-1056.....	623
GE5-1057.....	623
HAM Messages.....	624
HAM-1001.....	624
HAM-1002.....	624
HAM-1004.....	625
HAM-1005.....	626
HAM-1006.....	626
HAM-1007.....	626
HAM-1008.....	627
HAM-1009.....	627
HAM-1010.....	628
HAM-1011.....	628
HAM-1013.....	629
HAM-1014.....	629
HAM-1015.....	629
HAM-1016.....	630
HAM-1017.....	630
HAM-1018.....	631

HAM-1019.....	631
HAM-1020.....	631
HAM-1021.....	632
HAMK Messages.....	632
HAMK-1001.....	632
HAMK-1002.....	633
HAMK-1003.....	633
HAMK-1004.....	634
HIL Messages.....	634
HIL-1101.....	634
HIL-1102.....	634
HIL-1103.....	635
HIL-1104.....	635
HIL-1105.....	636
HIL-1106.....	636
HIL-1107.....	637
HIL-1108.....	637
HIL-1109.....	638
HIL-1201.....	638
HIL-1202.....	639
HIL-1203.....	639
HIL-1204.....	640
HIL-1206.....	640
HIL-1207.....	640
HIL-1208.....	641
HIL-1301.....	641
HIL-1302.....	642
HIL-1303.....	642
HIL-1304.....	643
HIL-1305.....	643
HIL-1306.....	644
HIL-1307.....	644
HIL-1308.....	644
HIL-1309.....	645
HIL-1310.....	645
HIL-1311.....	646
HIL-1312.....	646
HIL-1401.....	647
HIL-1402.....	647
HIL-1403.....	647

HIL-1404.....	648
HIL-1405.....	648
HIL-1501.....	649
HIL-1502.....	649
HIL-1503.....	650
HIL-1504.....	650
HIL-1505.....	651
HIL-1506.....	651
HIL-1507.....	652
HIL-1508.....	652
HIL-1509.....	653
HIL-1510.....	653
HIL-1511.....	654
HIL-1512.....	654
HIL-1513.....	655
HIL-1514.....	655
HIL-1515.....	656
HIL-1516.....	656
HIL-1517.....	657
HIL-1518.....	657
HIL-1519.....	658
HIL-1601.....	658
HIL-1602.....	659
HIL-1603.....	659
HIL-1605.....	659
HIL-1610.....	660
HIL-1611.....	660
HIL-1612.....	661
HIL-1613.....	661
HIL-1614.....	662
HIL-1615.....	662
HIL-1621.....	663
HIL-1623.....	663
HIL-1624.....	663
HIL-1625.....	664
HIL-1626.....	664
HIL-1627.....	665
HIL-1628.....	665
HIL-1629.....	666
HIL-1630.....	666

HIL-1650.....	666
HIL-1651.....	667
HIL-1652.....	667
HIL-1653.....	668
HIL-1654.....	668
HIL-1655.....	669
HIL-1656.....	669
HIL-1657.....	669
HIL-1658.....	670
HIL-1659.....	670
HIL-1660.....	671
HLO Messages.....	671
HLO-1001.....	671
HLO-1002.....	672
HLO-1003.....	672
HMON Messages.....	673
HMON-1001.....	673
HTTP Messages.....	673
HTTP-1001.....	673
HTTP-1002.....	674
HTTP-1003.....	674
HTTP-3001.....	675
HTTP-3002.....	675
HTTP-3003.....	676
HTTP-3004.....	676
HTTP-3005.....	676
HTTP-3006.....	677
HTTP-4001.....	677
IPAD Messages.....	678
IPAD-1000.....	678
IPAD-1001.....	678
IPAD-1002.....	679
IPAD-1003.....	679
IPAD-1004.....	679
IPAD-1005.....	680
IPAD-1006.....	680
IPAD-1007.....	681
ISNS Messages.....	681
ISNS-1001.....	681
ISNS-1002.....	682

ISNS-1003.....	682
ISNS-1004.....	682
ISNS-1005.....	683
ISNS-1006.....	683
ISNS-1008.....	683
ISNS-1009.....	684
ISNS-1010.....	684
ISNS-1011.....	685
ISNS-1013.....	685
ISNS-1014.....	686
KAC Messages.....	686
KAC-1002.....	686
KAC-1004.....	686
KAC-1006.....	687
KAC-1007.....	687
KAC-1008.....	688
KAC-1009.....	688
KAC-1010.....	689
KAC-1011.....	689
KAC-1012.....	689
KAC-1013.....	690
KAC-1014.....	690
KAC-1015.....	690
KAC-1016.....	691
KAC-1017.....	691
KAC-1018.....	692
KSWD Messages.....	692
KSWD-1001.....	692
KSWD-1002.....	693
KTRC Messages.....	693
KTRC-1001.....	693
KTRC-1002.....	693
KTRC-1003.....	694
KTRC-1004.....	694
KTRC-1005.....	695
KTRC-1006.....	695
LACP Messages.....	695
LACP-1001.....	695
LACP-1002.....	696
LACP-1003.....	696

LFM Messages.....	697
LFM-1001.....	697
LFM-1002.....	697
LFM-1003.....	697
LFM-1004.....	698
LFM-1005.....	698
LFM-1006.....	699
LFM-1007.....	699
LIC Messages.....	699
LIC-1000.....	699
LIC-1001.....	700
LIC-1002.....	700
LIC-1003.....	701
LIC-1004.....	701
LIC-1005.....	701
LIC-1009.....	702
LIC-1010.....	702
LIC-2000.....	703
LIC-2001.....	703
LIC-2002.....	704
LIC-2003.....	704
LOG Messages.....	704
LOG-1000.....	704
LOG-1001.....	705
LOG-1002.....	705
LOG-1003.....	706
LOG-1004.....	706
LOG-1005.....	706
LOG-1006.....	707
LOG-1007.....	707
LOG-1008.....	708
LOG-1009.....	708
LOG-1010.....	709
LOG-1011.....	709
LOG-1012.....	709
LOG-1013.....	710
LSDB Messages.....	710
LSDB-1001.....	710
LSDB-1002.....	711
LSDB-1003.....	711

LSDB-1004.....	712
LSDB-1005.....	712
MAPS Messages.....	712
MAPS-1001 to MAPS-1004.....	713
MAPS-1005.....	713
MAPS-1006.....	713
MAPS-1010.....	714
MAPS-1011.....	714
MAPS-1012.....	715
MAPS-1013.....	715
MAPS-1014.....	715
MAPS-1015.....	716
MAPS-1016.....	716
MAPS-1017.....	717
MAPS-1018.....	717
MAPS-1020.....	717
MAPS-1021.....	718
MAPS-1022.....	718
MAPS-1023.....	719
MAPS-1024.....	719
MAPS-1025.....	720
MAPS-1026.....	720
MAPS-1027.....	720
MAPS-1028.....	721
MAPS-1100.....	721
MAPS-1101.....	722
MAPS-1102.....	722
MAPS-1110.....	723
MAPS-1111.....	723
MAPS-1112.....	724
MAPS-1113.....	724
MAPS-1114.....	725
MAPS-1115.....	725
MAPS-1116.....	726
MAPS-1120.....	726
MAPS-1121.....	727
MAPS-1122.....	727
MAPS-1123.....	728
MAPS-1124.....	728
MAPS-1125.....	729

MAPS-1126.....	729
MAPS-1127.....	729
MAPS-1130.....	730
MAPS-1131.....	730
MAPS-1132.....	731
MAPS-1133.....	731
MAPS-1134.....	732
MAPS-1135.....	732
MAPS-1136.....	733
MAPS-1137.....	733
MAPS-1138.....	733
MAPS-1139.....	734
MAPS-1140.....	734
MAPS-1141.....	735
MAPS-1142.....	735
MAPS-1143.....	736
MAPS-1144.....	736
MAPS-1145.....	736
MAPS-1146.....	737
MAPS-1147.....	737
MAPS-1148.....	738
MAPS-1199.....	738
MAPS-1200.....	739
MAPS-1201.....	739
MAPS-1202.....	740
MAPS-1203.....	740
MAPS-1204.....	741
MAPS-1205.....	741
MAPS-1206.....	741
MAPS-1207.....	742
MAPS-1208.....	742
MAPS-1209.....	743
MAPS-1210.....	743
MAPS-1211.....	744
MAPS-1213.....	744
MAPS-1214.....	744
MAPS-1215.....	745
MAPS-1216.....	745
MAPS-1217.....	746
MAPS-1220.....	746

MAPS-1301.....	746
MAPS-1302.....	747
MAPS-2000.....	747
MAPS-2001.....	748
MAPS-2002.....	748
MAPS-2003.....	748
MAPS-2004 to MAPS-2007.....	749
MAPS-2008 to MAPS-2011.....	749
MAPS-2012 to MAPS-2015.....	750
MAPS-2016 to MAPS-2019.....	750
MAPS-2020 to MAPS-2023.....	750
MAPS-2024 to MAPS-2027.....	751
MAPS-2028 to MAPS-2031.....	751
MAPS-2032 to MAPS-2035.....	752
MAPS-2036 to MAPS-2039.....	752
MAPS-2040 to MAPS-2043.....	753
MAPS-2044 to MAPS-2047.....	753
MAPS-2048 to MAPS-2051.....	753
MAPS-2052 to MAPS-2055.....	754
MAPS-2056 to MAPS-2059.....	754
MAPS-2060 to MAPS-2063.....	755
MAPS-2064 to MAPS-2067.....	755
MAPS-2068 to MAPS-2071.....	755
MAPS-2072 to MAPS-2075.....	756
MAPS-2076 to MAPS-2079.....	756
MAPS-2080 to MAPS-2083.....	757
MAPS-2084 to MAPS-2087.....	757
MAPS-2088 to MAPS-2091.....	757
MAPS-2092 to MAPS-2095.....	758
MAPS-2096 to MAPS-2099.....	758
MAPS-2100 to MAPS-2103.....	759
MAPS-2104 to MAPS-2107.....	759
MAPS-2108 to MAPS-2111.....	760
MAPS-2112 to MAPS-2115.....	760
MAPS-2116 to MAPS-2119.....	760
MAPS-2120 to MAPS-2123.....	761
MAPS-2124 to MAPS-2127.....	761
MAPS-2128 to MAPS-2131.....	762
MAPS-2132 to MAPS-2135.....	762
MAPS-2136 to MAPS-2139.....	763

MAPS-2140 to MAPS-2143.....	763
MAPS-2144 to MAPS-2147.....	763
MAPS-2148 to MAPS-2151.....	764
MAPS-2152 to MAPS-2155.....	764
MAPS-2156 to MAPS-2159.....	765
MAPS-2160 to MAPS-2163.....	765
MAPS-2164 to MAPS-2167.....	766
MAPS-2168 to MAPS-2171.....	766
MAPS-2172 to MAPS-2175.....	767
MAPS-2176 to MAPS-2179.....	767
MAPS-2180 to MAPS-2183.....	767
MAPS-2184 to MAPS-2187.....	768
MAPS-2188 to MAPS-2191.....	768
MAPS-2192 to MAPS-2195.....	769
MAPS-2196 to MAPS-2199.....	769
MAPS-2200 to MAPS-2203.....	770
MAPS-2204 to MAPS-2207.....	770
MAPS-2208 to MAPS-2211.....	771
MAPS-2212 to MAPS-2215.....	771
MAPS-2216 to MAPS-2219.....	772
MAPS-2220 to MAPS-2223.....	772
MAPS-2224 to MAPS-2227.....	773
MAPS-2228 to MAPS-2231.....	773
MAPS-2232 to MAPS-2235.....	774
MAPS-2236 to MAPS-2239.....	774
MAPS-2240 to MAPS-2243.....	775
MAPS-2244 to MAPS-2247.....	775
MAPS-2248 to MAPS-2251.....	776
MAPS-2252 to MAPS-2255.....	776
MAPS-2256 to MAPS-2259.....	776
MAPS-2260 to MAPS-2263.....	777
MAPS-2264 to MAPS-2267.....	777
MAPS-2268 to MAPS-2271.....	778
MAPS-2272 to MAPS-2275.....	778
MAPS-2276 to MAPS-2279.....	779
MAPS-2280 to MAPS-2283.....	779
MAPS-2284 to MAPS-2287.....	780
MAPS-2288 to MAPS-2291.....	780
MAPS-2292 to MAPS-2295.....	780
MAPS-2296 to MAPS-2299.....	781

MAPS-2300 to MAPS-2303.....	781
MAPS-2304 to MAPS-2307.....	782
MAPS-2308 to MAPS-2311.....	782
MAPS-2312 to MAPS-2315.....	783
MAPS-2316 to MAPS-2319.....	783
MAPS-2320 to MAPS-2323.....	783
MAPS-2324 to MAPS-2327.....	784
MAPS-2328 to MAPS-2331.....	784
MAPS-2332 to MAPS-2335.....	785
MAPS-2336 to MAPS-2339.....	785
MAPS-2340 to MAPS-2343.....	786
MAPS-2344 to MAPS-2347.....	786
MAPS-2348 to MAPS-2351.....	787
MAPS-2352 to MAPS-2355.....	787
MAPS-2356 to MAPS-2359.....	788
MAPS-2360 to MAPS-2363.....	788
MAPS-2364 to MAPS-2367.....	788
MAPS-2368 to MAPS-2371.....	789
MAPS-2372 to MAPS-2375.....	789
MAPS-2376 to MAPS-2379.....	790
MAPS-2380 to MAPS-2383.....	790
MAPS-2384 to MAPS-2387.....	790
MAPS-2388 to MAPS-2391.....	791
MAPS-2392 to MAPS-2395.....	791
MAPS-2396 to MAPS-2399.....	791
MAPS-2400 to MAPS-2403.....	792
MAPS-2404 to MAPS-2407.....	792
MAPS-2408 to MAPS-2411.....	793
MAPS-2412 to MAPS-2415.....	793
MAPS-2416 to MAPS-2419.....	793
MAPS-2420 to MAPS-2423.....	794
MAPS-2424 to MAPS-2427.....	794
MAPS-2428 to MAPS-2431.....	795
MAPS-2432 to MAPS-2435.....	795
MAPS-2436 to MAPS-2439.....	796
MAPS-2440 to MAPS-2443.....	796
MAPS-2444 to MAPS-2447.....	796
MAPS-2448 to MAPS-2451.....	797
MAPS-2452 to MAPS-2455.....	797
MAPS-2456 to MAPS-2459.....	798

MAPS-2460 to MAPS-2463.....	798
MAPS-2464 to MAPS-2467.....	798
MAPS-2468 to MAPS-2471.....	799
MAPS-2472 to MAPS-2475.....	799
MAPS-2476 to MAPS-2479.....	799
MAPS-2480 to MAPS-2483.....	800
MAPS-2484 to MAPS-2487.....	800
MAPS-2488 to MAPS-2491.....	800
MAPS-2492 to MAPS-2495.....	801
MAPS-2496 to MAPS-2499.....	801
MAPS-2500 to MAPS-2503.....	802
MAPS-2504 to MAPS-2507.....	802
MAPS-2508 to MAPS-2511.....	802
MAPS-2512 to MAPS-2515.....	803
MAPS-2516 to MAPS-2519.....	803
MAPS-2520 to MAPS-2523.....	803
MAPS-2524 to MAPS-2527.....	804
MAPS-2528 to MAPS-2531.....	804
MAPS-2532 to MAPS-2535.....	804
MAPS-2536 to MAPS-2539.....	805
MAPS-2540 to MAPS-2543.....	805
MAPS-2544 to MAPS-2547.....	806
MAPS-2548 to MAPS-2551.....	806
MAPS-2552 to MAPS-2555.....	806
MAPS-2556 to MAPS-2559.....	807
MAPS-2560 to MAPS-2563.....	807
MAPS-2564 to MAPS-2567.....	807
MAPS-2568 to MAPS-2571.....	808
MAPS-2572 to MAPS-2575.....	808
MAPS-2576 to MAPS-2579.....	808
MAPS-2580 to MAPS-2583.....	809
MAPS-2584 to MAPS-2587.....	809
MAPS-2588 to MAPS-2591.....	810
MAPS-2592 to MAPS-2595.....	810
MAPS-2596 to MAPS-2599.....	810
MAPS-2600 to MAPS-2603.....	811
MAPS-2604 to MAPS-2607.....	811
MAPS-2608 to MAPS-2611.....	811
MAPS-2612 to MAPS-2615.....	812
MAPS-2616 to MAPS-2619.....	812

MAPS-2620 to MAPS-2623.....	812
MAPS-2624 to MAPS-2627.....	813
MAPS-2628 to MAPS-2631.....	813
MAPS-2640 to MAPS-2643.....	814
MAPS-2648 to MAPS-2651.....	814
MAPS-2652 to MAPS-2655.....	814
MAPS-2656 to MAPS-2659.....	815
MAPS-2660 to MAPS-2663.....	815
MAPS-2664 to MAPS-2667.....	815
MAPS-2668 to MAPS-2671.....	816
MAPS-2672 to MAPS-2675.....	816
MAPS-2676 to MAPS-2679.....	817
MAPS-2680 to MAPS-2683.....	817
MAPS-2684 to MAPS-2687.....	817
MAPS-2688 to MAPS-2691.....	818
MAPS-2692 to MAPS-2695.....	818
MAPS-2696 to MAPS-2699.....	818
MAPS-2700 to MAPS-2703.....	819
MAPS-2704 to MAPS-2707.....	819
MAPS-2708 to MAPS-2711.....	820
MAPS-2712 to MAPS-2715.....	820
MAPS-2716 to MAPS-2719.....	820
MAPS-2720 to MAPS-2723.....	821
MAPS-2724 to MAPS-2727.....	821
MAPS-2728 to MAPS-2731.....	822
MAPS-2732 to MAPS-2735.....	822
MAPS-2736 to MAPS-2739.....	822
MAPS-2740 to MAPS-2743.....	823
MAPS-2744 to MAPS-2747.....	823
MAPS-2748 to MAPS-2751.....	823
MAPS-2752 to MAPS-2755.....	824
MAPS-2756 to MAPS-2759.....	824
MAPS-2760 to MAPS-2763.....	824
MAPS-2764 to MAPS-2767.....	825
MAPS-2768 to MAPS-2771.....	825
MAPS-2772 to MAPS-2775.....	826
MAPS-2776 to MAPS-2779.....	826
MAPS-2780 to MAPS-2783.....	826
MAPS-2784 to MAPS-2787.....	827
MAPS-2788 to MAPS-2791.....	827

MAPS-2792 to MAPS-2795.....	827
MAPS-2796 to MAPS-2799.....	828
MAPS-2800 to MAPS-2803.....	828
MAPS-2804 to MAPS-2807.....	828
MAPS-2808 to MAPS-2811.....	829
MAPS-2812 to MAPS-2815.....	829
MAPS-2816 to MAPS-2819.....	830
MAPS-2820 to MAPS-2823.....	830
MAPS-2824 to MAPS-2827.....	830
MAPS-2828 to MAPS-2831.....	831
MAPS-2832 to MAPS-2835.....	831
MAPS-2836 to MAPS-2839.....	831
MAPS-2840 to MAPS-2843.....	832
MAPS-2844 to MAPS-2847.....	832
MAPS-2848 to MAPS-2851.....	832
MAPS-2852 to MAPS-2855.....	833
MAPS-2856 to MAPS-2859.....	833
MAPS-2860 to MAPS-2863.....	834
MAPS-2864 to MAPS-2867.....	834
MAPS-2868 to MAPS-2871.....	834
MAPS-2872 to MAPS-2875.....	835
MAPS-2876 to MAPS-2879.....	835
MAPS-2880 to MAPS-2883.....	835
MAPS-2884 to MAPS-2887.....	836
MAPS-2888 to MAPS-2891.....	836
MAPS-2892 to MAPS-2895.....	836
MAPS-2896 to MAPS-2899.....	837
MAPS-2900 to MAPS-2903.....	837
MAPS-2904 to MAPS-2907.....	838
MAPS-2908 to MAPS-2911.....	838
MAPS-2912 to MAPS-2915.....	838
MAPS-2916 to MAPS-2919.....	839
MAPS-2920 to MAPS-2923.....	839
MAPS-2924 to MAPS-2927.....	839
MAPS-2928 to MAPS-2931.....	840
MAPS-2932 to MAPS-2935.....	840
MAPS-2936 to MAPS-2939.....	840
MAPS-2940 to MAPS-2943.....	841
MAPS-2944 to MAPS-2947.....	841
MAPS-2948 to MAPS-2951.....	842

MAPS-2952 to MAPS-2955.....	842
MAPS-2956 to MAPS-2959.....	842
MAPS-2960 to MAPS-2963.....	843
MAPS-2964 to MAPS-2967.....	843
MAPS-2968 to MAPS-2971.....	843
MAPS-2972 to MAPS-2975.....	844
MAPS-2976 to MAPS-2979.....	844
MAPS-2980 to MAPS-2983.....	845
MAPS-2992 to MAPS-2995.....	845
MAPS-2996 to MAPS-2999.....	846
MAPS-3000 to MAPS-3003.....	846
MAPS-3004 to MAPS-3007.....	847
MAPS-3008 to MAPS-3011.....	847
MAPS-3016 to MAPS-3019.....	848
MAPS-3020 to MAPS-3023.....	848
MAPS-3024 to MAPS-3027.....	848
MAPS-3036 to MAPS-3039.....	849
MAPS-3040 to MAPS-3043.....	849
MAPS-3052 to MAPS-3055.....	850
MAPS-3056 to MAPS-3059.....	850
MAPS-3060 to MAPS-3063.....	851
MAPS-3064 to MAPS-3067.....	851
MAPS-3068 to MAPS-3071.....	852
MAPS-3072 to MAPS-3075.....	852
MAPS-3088 to MAPS-3091.....	853
MAPS-3092 to MAPS-3095.....	853
MAPS-3096 to MAPS-3099.....	854
MAPS-3120 to MAPS-3123.....	854
MAPS-3124 to MAPS-3127.....	855
MAPS-3128 to MAPS-3131.....	855
MAPS-3132 to MAPS-3135.....	856
MAPS-3136 to MAPS-3139.....	856
MAPS-3140 to MAPS-3143.....	857
MAPS-3144 to MAPS-3147.....	857
MAPS-3148 to MAPS-3151.....	857
MAPS-3152 to MAPS-3155.....	858
MAPS-3156 to MAPS-3159.....	858
MAPS-3184 to MAPS-3187.....	859
MAPS-3188 to MAPS-3191.....	859
MAPS-3192 to MAPS-3195.....	859

MAPS-3196 to MAPS-3199.....	860
MAPS-3200 to MAPS-3203.....	860
MAPS-3204 to MAPS-3207.....	860
MFIC Messages.....	861
MFIC-1001.....	861
MFIC-1002.....	861
MFIC-1003.....	862
MM Messages.....	862
MM-1001.....	862
MPTH Messages.....	863
MPTH-1003.....	863
MQ Messages.....	863
MQ-1004.....	863
MQ-1005.....	864
MQ-1006.....	864
MQ-1007.....	865
MS Messages.....	865
MS-1001.....	865
MS-1002.....	866
MS-1003.....	866
MS-1004.....	867
MS-1005.....	867
MS-1006.....	868
MS-1008.....	868
MS-1009.....	869
MS-1021.....	869
MS-1022.....	870
MS-1023.....	870
MS-1024.....	870
MS-1025.....	871
MS-1026.....	871
MS-1027.....	872
MS-1028.....	872
MS-1029.....	872
MS-1030.....	873
MS-1031.....	873
NBFS Messages.....	874
NBFS-1001.....	874
NBFS-1002.....	874
NBFS-1003.....	875

NBFS-1004.....	876
NBFS-1005.....	876
NBFS-1006.....	877
NS Messages.....	877
NS-1001.....	878
NS-1002.....	878
NS-1003.....	879
NS-1004.....	879
NS-1009.....	880
NS-1010.....	880
NS-1012.....	880
NS-1013.....	881
NS-1014.....	881
NS-1015.....	882
NS-1016.....	882
NS-1017.....	883
NS-1018.....	883
NS-1020.....	884
NS-1021.....	884
NS-1022.....	884
NS-1023.....	885
NS-1024.....	885
NS-1025.....	886
NS-1026.....	886
NS-1027.....	887
LLDP Messages.....	887
LLDP-1000.....	887
LLDP-1001.....	887
LLDP-1002.....	888
LLDP-1003.....	888
LLDP-1004.....	888
LLDP-1005.....	889
PDM Messages.....	889
PDM-1001.....	889
PDM-1002.....	890
PDM-1003.....	890
PDM-1004.....	891
PDM-1005.....	891
PDM-1006.....	891
PDM-1007.....	892

PDM-1008.....	892
PDM-1009.....	893
PDM-1010.....	893
PDM-1011.....	894
PDM-1012.....	894
PDM-1013.....	895
PDM-1014.....	895
PDM-1017.....	896
PDM-1019.....	896
PDM-1020.....	896
PDM-1021.....	897
PDM-1022.....	897
PDM-1023.....	898
PDM-1024.....	898
PDM-1025.....	899
PDM-1026.....	899
PDM-1027.....	899
PDM-1028.....	900
PDTR Messages.....	900
PDTR-1001.....	900
PDTR-1002.....	901
PLAT Messages.....	901
PLAT-1000.....	901
PLAT-1001.....	902
PLAT-1002.....	902
PLAT-1003.....	903
PLAT-1004.....	903
PLAT-1005.....	904
PLAT-1006.....	904
PLAT-1007.....	904
PLAT-1008.....	905
PLAT-1009.....	905
PLAT-1010.....	906
PLAT-1011.....	906
PLAT-1072.....	907
PLAT-1073.....	907
PLAT-1100.....	908
PLAT-2000.....	908
PLAT-2001.....	908
PMGR Messages.....	909

PMGR-1001.....	909
PMGR-1002.....	909
PMGR-1003.....	910
PMGR-1004.....	910
PMGR-1005.....	911
PMGR-1006.....	911
PMGR-1007.....	911
PMGR-1008.....	912
PMGR-1009.....	912
PMGR-1010.....	913
PMGR-1011.....	913
PMGR-1012.....	913
PMGR-1013.....	914
PMGR-1014.....	914
PORT Messages.....	915
PORT-1003.....	915
PORT-1004.....	915
PORT-1005.....	916
PORT-1006.....	916
PORT-1007.....	917
PORT-1008.....	917
PORT-1009.....	917
PORT-1010.....	918
PORT-1011.....	918
PORT-1012.....	919
PORT-1013.....	919
PORT-1014.....	919
PORT-1015.....	920
PORT-1016.....	920
PORT-1017.....	921
PORT-1018.....	921
PORT-1019.....	921
PORT-1020.....	922
PORT-1021.....	922
PORT-1022.....	923
PORT-1023.....	923
PORT-1024.....	923
PORT-1025.....	924
PORT-1026.....	924
PORT-1027.....	925

PORT-1028.....	925
PORT-1029.....	925
PORT-1030.....	926
PORT-1031.....	926
PORT-1032.....	927
PORT-1033.....	927
PORT-1034.....	927
PORT-1035.....	928
PORT-1036.....	928
PORT-1037.....	929
PORT-1038.....	929
PORT-1039.....	929
PORT-1040.....	930
PORT-1041.....	930
PORT-1042.....	931
PORT-1043.....	931
PORT-1044.....	931
PORT-1045.....	932
PORT-1046.....	932
PORT-1047.....	933
PORT-1048.....	933
PORT-1049.....	933
PORT-1050.....	934
PORT-1051.....	934
PORT-1052.....	935
PORT-1053.....	935
PORT-1054.....	935
PORT-1055.....	936
PORT-1056.....	936
PORT-1057.....	937
PORT-1058.....	937
PORT-1059.....	938
PORT-1060.....	938
PORT-1061.....	938
PORT-1062.....	939
PORT-1063.....	939
PORT-1064.....	940
PORT-1065.....	940
PORT-1066.....	940
PORT-1067.....	941

PORT-1068.....	941
PORT-1069.....	942
PORT-1070.....	942
PORT-1071.....	942
PORT-1072.....	943
PORT-1073.....	943
PORT-1074.....	944
PORT-1075.....	944
PORT-1076.....	944
PORT-1077.....	945
PORT-1078.....	945
PORT-1079.....	946
PORT-1080.....	946
PORT-1081.....	946
PORT-1082.....	947
PS Messages.....	947
PS-1000.....	947
PS-1001.....	948
PS-1002.....	948
PS-1009.....	949
PSWP Messages.....	949
PSWP-1001.....	949
PSWP-1002.....	949
PSWP-1003.....	950
PSWP-1004.....	950
PSWP-1005.....	951
PSWP-1006.....	951
PSWP-1007.....	951
PSWP-1008.....	952
RAS Messages.....	952
RAS-1001.....	952
RAS-1002.....	953
RAS-1003.....	953
RAS-1004.....	954
RAS-1005.....	954
RAS-1006.....	954
RAS-1007.....	955
RAS-1008.....	955
RAS-1009.....	956
RAS-1010.....	956

RAS-1011.....	956
RAS-1012.....	957
RAS-1013.....	957
RAS-1014.....	958
RAS-1015.....	958
RAS-1016.....	958
RAS-2001.....	959
RAS-2002.....	959
RAS-2003.....	960
RAS-2004.....	960
RAS-2005.....	960
RAS-2006.....	961
RAS-2007.....	961
RAS-2008.....	962
RAS-2009.....	962
RAS-2010.....	962
RAS-2011.....	963
RAS-2012.....	963
RAS-2013.....	964
RAS-2014.....	964
RAS-2015.....	964
RAS-3001.....	965
RAS-3002.....	965
RAS-3003.....	966
RAS-3004.....	966
RAS-3005.....	966
RAS-3006.....	967
RAS-3007.....	967
RAS-3008.....	968
RAS-3009.....	968
RCS Messages.....	968
RCS-1001.....	969
RCS-1002.....	969
RCS-1003.....	969
RCS-1004.....	970
RCS-1005.....	970
RCS-1006.....	971
RCS-1007.....	971
RCS-1008.....	972
RCS-1009.....	972

RCS-1011.....	973
RCS-1012.....	973
RCS-1013.....	974
RCS-1014.....	974
RPCD Messages.....	974
RPCD-1001.....	974
RPCD-1002.....	975
RPCD-1003.....	975
RPCD-1004.....	976
RPCD-1005.....	976
RPCD-1006.....	976
RPCD-1007.....	977
RTE Messages.....	977
RTE-1001.....	977
RTE-1002.....	978
RTE-1003.....	978
RTE-1004.....	979
RTE-1005.....	979
RTWR Messages.....	979
RTWR-1001.....	980
RTWR-1002.....	980
RTWR-1003.....	981
RTWR-1004.....	981
SCN Messages.....	982
SCN-1001.....	982
SCN-1002.....	982
SEC Messages.....	983
SEC-1001.....	983
SEC-1002.....	984
SEC-1003.....	984
SEC-1005.....	985
SEC-1006.....	985
SEC-1007.....	986
SEC-1008.....	986
SEC-1009.....	987
SEC-1010.....	987
SEC-1016.....	988
SEC-1022.....	988
SEC-1024.....	988
SEC-1025.....	989

SEC-1026.....	989
SEC-1028.....	990
SEC-1029.....	990
SEC-1030.....	991
SEC-1031.....	991
SEC-1032.....	992
SEC-1033.....	992
SEC-1034.....	993
SEC-1035.....	993
SEC-1036.....	993
SEC-1037.....	994
SEC-1038.....	994
SEC-1039.....	995
SEC-1040.....	995
SEC-1041.....	995
SEC-1042.....	996
SEC-1043.....	996
SEC-1044.....	997
SEC-1045.....	997
SEC-1046.....	998
SEC-1049.....	998
SEC-1050.....	999
SEC-1051.....	999
SEC-1052.....	1000
SEC-1053.....	1000
SEC-1054.....	1001
SEC-1055.....	1001
SEC-1056.....	1002
SEC-1057.....	1002
SEC-1059.....	1003
SEC-1062.....	1003
SEC-1063.....	1003
SEC-1064.....	1004
SEC-1065.....	1004
SEC-1069.....	1005
SEC-1071.....	1005
SEC-1072.....	1006
SEC-1073.....	1006
SEC-1074.....	1006
SEC-1075.....	1007

SEC-1076.....	1007
SEC-1077.....	1008
SEC-1078.....	1008
SEC-1079.....	1009
SEC-1080.....	1009
SEC-1081.....	1010
SEC-1082.....	1010
SEC-1083.....	1010
SEC-1084.....	1011
SEC-1085.....	1011
SEC-1086.....	1012
SEC-1087.....	1012
SEC-1088.....	1012
SEC-1089.....	1013
SEC-1090.....	1013
SEC-1091.....	1014
SEC-1092.....	1014
SEC-1093.....	1015
SEC-1094.....	1015
SEC-1095.....	1016
SEC-1096.....	1016
SEC-1097.....	1016
SEC-1098.....	1017
SEC-1099.....	1017
SEC-1100.....	1018
SEC-1101.....	1018
SEC-1102.....	1019
SEC-1104.....	1019
SEC-1105.....	1020
SEC-1106.....	1020
SEC-1107.....	1020
SEC-1108.....	1021
SEC-1110.....	1021
SEC-1111.....	1022
SEC-1112.....	1022
SEC-1113.....	1023
SEC-1114.....	1023
SEC-1115.....	1024
SEC-1116.....	1024
SEC-1117.....	1025

SEC-1118.....	1025
SEC-1119.....	1025
SEC-1121.....	1026
SEC-1122.....	1026
SEC-1123.....	1027
SEC-1124.....	1027
SEC-1126.....	1027
SEC-1130.....	1028
SEC-1135.....	1028
SEC-1136.....	1029
SEC-1137.....	1029
SEC-1138.....	1030
SEC-1139.....	1030
SEC-1142.....	1031
SEC-1145.....	1031
SEC-1146.....	1032
SEC-1153.....	1032
SEC-1154.....	1032
SEC-1155.....	1033
SEC-1156.....	1033
SEC-1157.....	1034
SEC-1158.....	1034
SEC-1159.....	1035
SEC-1160.....	1035
SEC-1163.....	1036
SEC-1164.....	1036
SEC-1165.....	1036
SEC-1166.....	1037
SEC-1167.....	1037
SEC-1168.....	1038
SEC-1170.....	1038
SEC-1171.....	1039
SEC-1172.....	1039
SEC-1173.....	1040
SEC-1174.....	1040
SEC-1175.....	1040
SEC-1176.....	1041
SEC-1180.....	1041
SEC-1181.....	1042
SEC-1182.....	1042

SEC-1183.....	1042
SEC-1184.....	1043
SEC-1185.....	1043
SEC-1186.....	1044
SEC-1187.....	1044
SEC-1188.....	1044
SEC-1189.....	1045
SEC-1190.....	1045
SEC-1191.....	1046
SEC-1192.....	1046
SEC-1193.....	1047
SEC-1194.....	1047
SEC-1195.....	1048
SEC-1196.....	1048
SEC-1197.....	1049
SEC-1198.....	1049
SEC-1199.....	1049
SEC-1200.....	1050
SEC-1201.....	1050
SEC-1202.....	1051
SEC-1203.....	1051
SEC-1250.....	1052
SEC-1251.....	1052
SEC-1253.....	1053
SEC-1300.....	1053
SEC-1301.....	1054
SEC-1302.....	1054
SEC-1303.....	1054
SEC-1304.....	1055
SEC-1305.....	1055
SEC-1306.....	1056
SEC-1307.....	1056
SEC-1308.....	1057
SEC-1309.....	1057
SEC-1310.....	1058
SEC-1311.....	1058
SEC-1312.....	1059
SEC-1313.....	1059
SEC-1314.....	1059
SEC-1315.....	1060

SEC-1316.....	1060
SEC-1317.....	1061
SEC-1318.....	1061
SEC-1319.....	1062
SEC-1320.....	1062
SEC-1321.....	1062
SEC-1322.....	1063
SEC-1323.....	1063
SEC-1324.....	1064
SEC-1325.....	1064
SEC-1326.....	1065
SEC-1327.....	1065
SEC-1328.....	1065
SEC-1329.....	1066
SEC-1330.....	1066
SEC-1331.....	1067
SEC-1332.....	1067
SEC-1333.....	1068
SEC-1334.....	1068
SEC-1335.....	1068
SEC-1336.....	1069
SEC-1337.....	1069
SEC-1338.....	1070
SEC-1339.....	1070
SEC-1340.....	1071
SEC-1341.....	1071
SEC-1342.....	1072
SEC-1343.....	1072
SEC-1344.....	1072
SEC-1345.....	1073
SEC-1346.....	1073
SEC-1347.....	1074
SEC-1348.....	1074
SEC-1349.....	1075
SEC-1350.....	1075
SEC-1351.....	1075
SEC-1352.....	1076
SEC-3001.....	1076
SEC-3002.....	1077
SEC-3003.....	1077

SEC-3004.....	1078
SEC-3005.....	1078
SEC-3006.....	1079
SEC-3007.....	1079
SEC-3008.....	1080
SEC-3009.....	1080
SEC-3010.....	1081
SEC-3011.....	1081
SEC-3012.....	1082
SEC-3013.....	1082
SEC-3014.....	1083
SEC-3015.....	1083
SEC-3016.....	1084
SEC-3018.....	1085
SEC-3019.....	1085
SEC-3020.....	1086
SEC-3021.....	1086
SEC-3022.....	1087
SEC-3023.....	1087
SEC-3024.....	1088
SEC-3025.....	1088
SEC-3026.....	1089
SEC-3027.....	1089
SEC-3028.....	1090
SEC-3029.....	1090
SEC-3030.....	1091
SEC-3031.....	1091
SEC-3032.....	1092
SEC-3033.....	1092
SEC-3034.....	1093
SEC-3035.....	1093
SEC-3036.....	1094
SEC-3037.....	1094
SEC-3038.....	1095
SEC-3039.....	1095
SEC-3043.....	1096
SEC-3044.....	1096
SEC-3045.....	1097
SEC-3046.....	1097
SEC-3047.....	1098

SEC-3048.....	1098
SEC-3049.....	1099
SEC-3050.....	1099
SEC-3051.....	1100
SEC-3061.....	1100
SEC-3062.....	1100
SEC-3063.....	1101
SEC-3064.....	1101
SEC-3065.....	1102
SEC-3066.....	1102
SEC-3067.....	1102
SEC-3068.....	1103
SEC-3069.....	1103
SEC-3070.....	1104
SEC-3071.....	1104
SEC-3072.....	1105
SEC-3073.....	1105
SEC-3074.....	1106
SEC-3075.....	1106
SEC-3076.....	1107
SEC-3077.....	1107
SEC-3078.....	1108
SEC-3079.....	1108
SEC-3080.....	1109
SEC-3081.....	1109
SEC-3082.....	1110
SEC-3083.....	1110
SEC-3085.....	1110
SEC-3086.....	1111
SEC-3087.....	1111
SEC-3088.....	1112
SEC-3089.....	1112
SEC-3090.....	1113
SEC-3091.....	1113
SEC-3092.....	1114
SEC-3093.....	1114
SEC-3094.....	1115
SEC-3095.....	1115
SEC-3096.....	1116
SEC-3097.....	1116

SLNK Messages.....	1117
SLNK-1001.....	1117
SLNK-1002.....	1117
SLNK-1003.....	1118
SLNK-1005.....	1118
SNMP Messages.....	1118
SNMP-1001.....	1119
SNMP-1002.....	1119
SNMP-1003.....	1119
SNMP-1004.....	1120
SNMP-1005.....	1120
SNMP-1006.....	1121
SNMP-1009.....	1121
SNMP-1010.....	1122
SNMP-1011.....	1122
SNMP-1012.....	1123
SNMP-1013.....	1123
SNMP-3020.....	1124
SPM Messages.....	1124
SPM-1001.....	1124
SPM-1002.....	1125
SPM-1003.....	1125
SPM-1004.....	1125
SPM-1005.....	1126
SPM-1006.....	1126
SPM-1007.....	1126
SPM-1008.....	1127
SPM-1009.....	1127
SPM-1010.....	1127
SPM-1011.....	1128
SPM-1012.....	1128
SPM-1013.....	1129
SPM-1014.....	1129
SPM-1015.....	1129
SPM-1016.....	1130
SPM-3001.....	1130
SPM-3002.....	1131
SPM-3003.....	1131
SPM-3004.....	1132
SPM-3005.....	1132

SPM-3006.....	1132
SPM-3007.....	1133
SPM-3008.....	1133
SPM-3009.....	1134
SPM-3010.....	1134
SPM-3011.....	1134
SPM-3012.....	1135
SPM-3013.....	1135
SPM-3014.....	1136
SPM-3015.....	1136
SPM-3016.....	1136
SPM-3017.....	1137
SPM-3018.....	1137
SPM-3019.....	1138
SPM-3020.....	1138
SPM-3021.....	1139
SPM-3022.....	1139
SPM-3023.....	1139
SPM-3024.....	1140
SPM-3025.....	1140
SPM-3026.....	1141
SPM-3027.....	1141
SPM-3028.....	1141
SPM-3029.....	1142
SRM Messages.....	1142
SRM-1001.....	1142
SRM-1001.....	1143
SRM-1002.....	1143
SRM-1002.....	1143
SRM-2001.....	1144
SRM-2001.....	1144
SS Messages.....	1145
SS-1000.....	1145
SS-1001.....	1145
SS-1002.....	1146
SS-1003.....	1146
SS-1004.....	1146
SS-1005.....	1147
SS-1006.....	1147
SS-1007.....	1148

SS-1008.....	1148
SS-1009.....	1149
SS-1010.....	1149
SS-1011.....	1149
SS-1012.....	1150
SS-1013.....	1150
SS-1014.....	1151
SS-1015.....	1151
SS-1016.....	1151
SSLP Messages.....	1152
SSLP-1001.....	1152
SULB Messages.....	1152
SULB-1001.....	1152
SULB-1002.....	1153
SULB-1003.....	1153
SULB-1004.....	1154
SULB-1005.....	1154
SULB-1006.....	1155
SULB-1007.....	1155
SULB-1008.....	1156
SULB-1009.....	1156
SULB-1010.....	1163
SULB-1011.....	1163
SULB-1017.....	1164
SULB-1018.....	1164
SULB-1020.....	1165
SULB-1021.....	1165
SULB-1022.....	1166
SULB-1023.....	1166
SULB-1024.....	1167
SULB-1025.....	1167
SULB-1026.....	1168
SULB-1030.....	1168
SULB-1031.....	1169
SULB-1032.....	1169
SULB-1033.....	1170
SULB-1034.....	1170
SULB-1035.....	1171
SULB-1036.....	1171
SULB-1037.....	1172

SULB-1039.....	1172
SULB-1040.....	1173
SULB-1041.....	1173
SULB-1042.....	1174
SULB-1043.....	1174
SULB-1044.....	1175
SULB-1050.....	1175
SULB-1051.....	1176
SULB-1052.....	1176
SULB-1053.....	1177
SULB-1054.....	1177
SULB-1055.....	1177
SULB-1056.....	1178
SULB-1060.....	1178
SULB-1061.....	1179
SULB-1062.....	1179
SULB-1063.....	1180
SULB-1064.....	1180
SULB-1065.....	1181
SULB-1066.....	1181
SULB-1067.....	1182
SWCH Messages.....	1182
SWCH-1001.....	1182
SWCH-1002.....	1183
SWCH-1003.....	1183
SWCH-1004.....	1184
SWCH-1005.....	1184
SWCH-1006.....	1185
SWCH-1007.....	1185
SWCH-1008.....	1186
SWCH-1009.....	1186
SWCH-1010.....	1187
SWCH-1011.....	1187
SWCH-1012.....	1187
SWCH-1013.....	1188
SWCH-1014.....	1188
SWCH-1015.....	1189
SWCH-1016.....	1189
SWCH-1017.....	1190
SWCH-1018.....	1190

SWCH-1019.....	1191
SWCH-1020.....	1191
SWCH-1021.....	1192
SWCH-1022.....	1192
SWCH-1023.....	1192
SWCH-1024.....	1193
SWCH-1025.....	1193
SWCH-1026.....	1194
SWCH-1027.....	1194
SWCH-1028.....	1195
SWCH-1029.....	1195
SWCH-1030.....	1195
SWCH-1031.....	1196
SWCH-1032.....	1196
SWCH-1033.....	1197
SWCH-1034.....	1197
SWCH-1035.....	1197
SWCH-1036.....	1198
SWCH-1037.....	1198
SWCH-1038.....	1199
SWCH-1039.....	1199
SWCH-1040.....	1199
SWCH-1041.....	1200
SWCH-1042.....	1200
SWCH-1043.....	1201
SWCH-1044.....	1201
SWCH-1045.....	1201
SWCH-1046.....	1202
SWCH-1047.....	1202
SWCH-1048.....	1203
SWCH-1049.....	1203
SWCH-1050.....	1204
SWCH-1051.....	1204
SWCH-1052.....	1204
SWCH-1053.....	1205
SWCH-1060.....	1205
SWCH-1061.....	1206
SWCH-1062.....	1206
SWCH-1063.....	1207
SWCH-1064.....	1207

SWCH-1065.....	1208
SYSC Messages.....	1208
SYSC-1001.....	1208
SYSC-1002.....	1209
SYSC-1004.....	1209
SYSC-1005.....	1209
SYSM Messages.....	1210
SYSM-1001.....	1210
SYSM-1002.....	1210
SYSM-1003.....	1211
SYSM-1004.....	1211
SYSM-1005.....	1212
SYSM-1006.....	1212
SYSM-1007.....	1213
SYSM-1008.....	1213
TO Messages.....	1213
TO-1001.....	1214
TO-1005.....	1214
TO-1006.....	1214
TO-1007.....	1215
TO-1008.....	1215
TO-1009.....	1216
TO-1010.....	1216
TO-1011.....	1216
TO-1012.....	1217
TO-1013.....	1217
TO-1014.....	1218
TO-1015.....	1218
TO-1016.....	1219
TO-1017.....	1219
TO-1018.....	1219
TO-1019.....	1220
TO-1020.....	1220
TO-3001.....	1221
TRCE Messages.....	1221
TRCE-1001.....	1221
TRCE-1002.....	1222
TRCE-1003.....	1222
TRCE-1004.....	1223
TRCE-1005.....	1223

TRCE-1006.....	1223
TRCE-1007.....	1224
TRCE-1008.....	1224
TRCE-1009.....	1225
TRCE-1010.....	1225
TRCE-1011.....	1226
TRCE-1012.....	1226
TRCE-1013.....	1227
TS Messages.....	1227
TS-1001.....	1227
TS-1002.....	1228
TS-1006.....	1228
TS-1007.....	1229
TS-1008.....	1229
TS-1009.....	1230
TS-1010.....	1230
TS-1011.....	1230
TS-1012.....	1231
TS-1013.....	1231
TS-1014.....	1232
TS-1015.....	1232
TS-1016.....	1232
TS-1017.....	1233
TS-1018.....	1233
TS-1019.....	1234
TS-1020.....	1234
UCID Messages.....	1235
UCID-1001.....	1235
UCID-3001.....	1235
UCID-3002.....	1236
UCID-3003.....	1236
UCID-3004.....	1236
UCID-3005.....	1237
UCID-3006.....	1237
UCID-3007.....	1238
UCID-3008.....	1238
UCID-3009.....	1238
UCID-3010.....	1239
UCID-3011.....	1239
UCID-3012.....	1240

UCID-3013.....	1240
UCID-3014.....	1240
UCID-3015.....	1241
UCID-3016.....	1241
UCID-3017.....	1242
UCID-3018.....	1242
UCID-3019.....	1242
UCID-3020.....	1243
UCID-3021.....	1243
UCID-3022.....	1244
UCID-3023.....	1244
UCID-3025.....	1244
UCID-3026.....	1245
UCID-3027.....	1245
UCID-3028.....	1246
UCID-3029.....	1246
UCID-3030.....	1246
UCID-3031.....	1247
UCID-3032.....	1247
UCID-3033.....	1248
UCID-3034.....	1248
UCID-3035.....	1248
UCID-3036.....	1249
UCID-3037.....	1249
UCID-3038.....	1250
UCID-3039.....	1250
UCID-3040.....	1250
UCID-3041.....	1251
UCID-3042.....	1251
UCID-3043.....	1252
UCID-3044.....	1252
UCID-3045.....	1252
UCID-3046.....	1253
UCID-3047.....	1253
UCID-3048.....	1254
UCID-3049.....	1254
UCID-3050.....	1254
UCID-3051.....	1255
UCID-3052.....	1255
UCID-3053.....	1256

UCID-3054.....	1256
UCID-3055.....	1256
UCID-3056.....	1257
UCST Messages.....	1257
UCST-1003.....	1257
UCST-1007.....	1258
UCST-1020.....	1258
UCST-1021.....	1258
UCST-1022.....	1259
UCST-1023.....	1259
UCST-1024.....	1260
UCST-1026.....	1260
UCST-1027.....	1261
UCST-1028.....	1261
UCST-1029.....	1261
UCST-1030.....	1262
UCST-1031.....	1262
UCST-1032.....	1263
UCST-1033.....	1263
UFCS Messages.....	1263
UFCS-1001.....	1263
UFCS-1002.....	1264
UFCS-1003.....	1264
UFCS-1004.....	1265
UFCS-1005.....	1265
UFCS-2004.....	1266
UFCS-2005.....	1266
UFCS-2006.....	1267
UFCS-2007.....	1267
UFCS-2008.....	1267
UFCS-2009.....	1268
UPTH Messages.....	1268
UPTH-1001.....	1268
UPTH-1002.....	1269
USL Messages.....	1269
USL-1001.....	1269
USL-1002.....	1270
USL-1003.....	1270
USL-1004.....	1271
USL-1005.....	1271

USL-1006.....	1272
USL-1007.....	1272
USL-1008.....	1272
USL-1009.....	1273
USL-1010.....	1273
USL-1011.....	1273
USL-1012.....	1274
USL-1013.....	1274
USL-1014.....	1274
USL-1015.....	1275
USL-1016.....	1275
USL-1017.....	1275
USL-1018.....	1276
USL-1019.....	1276
USL-1020.....	1276
VS Messages.....	1277
VS-1001.....	1277
VS-1002.....	1277
VS-1003.....	1277
VS-1004.....	1278
VS-1005.....	1278
VS-1006.....	1279
VS-1007.....	1279
VS-1008.....	1279
WEBD Messages.....	1280
WEBD-1001.....	1280
WEBD-1002.....	1280
WEBD-1004.....	1281
WEBD-1005.....	1281
WEBD-1006.....	1281
WEBD-1007.....	1282
WEBD-1008.....	1282
WEBD-1009.....	1282
XTUN Messages.....	1283
XTUN-1000.....	1283
XTUN-1001.....	1283
XTUN-1002.....	1284
XTUN-1003.....	1284
XTUN-1004.....	1285
XTUN-1005.....	1285

XTUN-1006.....	1285
XTUN-1007.....	1286
XTUN-1008.....	1286
XTUN-1009.....	1287
XTUN-1010.....	1287
XTUN-1996.....	1288
XTUN-1997.....	1288
XTUN-2012.....	1289
XTUN-2013.....	1289
XTUN-2014.....	1289
XTUN-2015.....	1290
XTUN-3000.....	1290
XTUN-3001.....	1291
XTUN-3002.....	1291
XTUN-3003.....	1291
XTUN-3004.....	1292
XTUN-3005.....	1292
XTUN-3006.....	1292
XTUN-3007.....	1293
XTUN-3008.....	1293
XTUN-3009.....	1294
XTUN-3010.....	1294
XTUN-3100.....	1294
XTUN-3101.....	1295
XTUN-3102.....	1295
ZONE Messages.....	1296
ZONE-1003.....	1296
ZONE-1004.....	1296
ZONE-1007.....	1297
ZONE-1010.....	1297
ZONE-1015.....	1298
ZONE-1017.....	1298
ZONE-1019.....	1298
ZONE-1022.....	1299
ZONE-1023.....	1299
ZONE-1024.....	1300
ZONE-1026.....	1300
ZONE-1027.....	1301
ZONE-1028.....	1301
ZONE-1029.....	1302

ZONE-1034.....	1302
ZONE-1036.....	1303
ZONE-1037.....	1303
ZONE-1038.....	1303
ZONE-1039.....	1304
ZONE-1040.....	1304
ZONE-1041.....	1305
ZONE-1042.....	1305
ZONE-1043.....	1306
ZONE-1044.....	1306
ZONE-1045.....	1307
ZONE-1046.....	1307
ZONE-1048.....	1307
ZONE-1049.....	1308
ZONE-1054.....	1308
ZONE-1059.....	1309
ZONE-1061.....	1309
ZONE-1062.....	1309
ZONE-1064.....	1310
ZONE-1065.....	1310
ZONE-1066.....	1311
ZONE-1067.....	1311
ZONE-1068.....	1312
ZONE-1069.....	1312
ZONE-1070.....	1312
ZONE-1071.....	1313
ZONE-1072.....	1313
ZONE-1073.....	1314
ZONE-1074.....	1314
ZONE-1075.....	1315
ZONE-1076.....	1315
ZONE-1077.....	1315
ZONE-1078.....	1316
ZONE-1079.....	1316
ZONE-1080.....	1317
ZONE-1081.....	1317
ZONE-1082.....	1318
ZONE-1083.....	1318
ZONE-1084.....	1319
ZONE-1085.....	1319

ZONE-1086.....	1320
ZONE-1087.....	1320
ZONE-1088.....	1320
ZONE-1089.....	1321
ZONE-1090.....	1321
ZONE-1091.....	1322
ZONE-1092.....	1322
ZONE-1093.....	1323
ZONE-1094.....	1323
ZONE-1095.....	1324
ZONE-1096.....	1324
ZONE-1097.....	1324
ZONE-1098.....	1325
ZONE-3001.....	1325
ZONE-3002.....	1326
ZONE-3003.....	1327
ZONE-3004.....	1327
ZONE-3005.....	1328
ZONE-3006.....	1328
ZONE-3007.....	1329
ZONE-3008.....	1329
ZONE-3009.....	1330
ZONE-3010.....	1330
ZONE-3011.....	1331
ZONE-3012.....	1331
ZONE-3026.....	1332
ZONE-3027.....	1332
ZONE-3028.....	1333
ZONE-3029.....	1333
ZONE-3030.....	1334
ZONE-3031.....	1334
ZONE-3032.....	1335
ZONE-3033.....	1335
ZONE-3034.....	1336
MAPS Monitoring Systems and RASLog IDs.....	1337
Revision History.....	1341
Documentation Legal Notice.....	1342

Introduction

This manual supports Fabric OS® v9.2.x and later and documents system messages that can help you diagnose and fix problems with a switch or fabric. The messages in this manual are organized alphabetically by module name. A *module* is a subsystem in the Fabric OS software. Each module generates a set of numbered messages. For each message, this manual provides the message text, message type, severity level, probable cause, and recommended action. There may be more than one cause and more than one recommended action for any given message. This manual discusses the most probable cause and the typical recommended action.

Supported Hardware and Software

The following hardware platforms are supported by Brocade Fabric OS v9.2.x.

Brocade Gen 7 (64G) Fixed-Port Switches

- Brocade G720 Switch
- Brocade G730 Switch
- Brocade 7850 Extension Switch

Brocade Gen 7 (64G) Directors

For ease of reference, Brocade chassis-based storage systems are standardizing on the term *director*. The legacy term *backbone* can be used interchangeably with the term *director*.

- Brocade X7-4 Director
- Brocade X7-8 Director

Brocade Gen 6 (32G) Fixed-Port Switches

- Brocade G610 Switch
- Brocade G620 Switch
- Brocade G630 Switch
- Brocade 7810 Extension Switch
- Brocade G648 Blade Server SAN I/O Module
- Brocade MXG610 Blade Server SAN I/O Module

Brocade Gen 6 (32G) Directors

- Brocade X6-4 Director
- Brocade X6-8 Director

Contacting Technical Support for Your Brocade® Product

If you purchased Brocade® product support from a Broadcom® OEM or solution provider, contact your OEM or solution provider for all your product support needs.

- OEM and solution providers are trained and certified by Broadcom to support Brocade products.
- Broadcom provides backline support for issues that cannot be resolved by the OEM or solution provider.
- Brocade Supplemental Support augments your existing OEM support contract, providing direct access to Brocade expertise. For more information on this option, contact Broadcom or your OEM.
- For questions regarding service levels and response times, contact your OEM or solution provider.

If you purchased Brocade product support directly from Broadcom, use one of the following methods to contact the Technical Assistance Center 24x7. For product support information and the latest information on contacting the Technical Assistance Center, go to www.broadcom.com/support/fibre-channel-networking/contact-brocade-support.

Online	Telephone
For nonurgent issues, the preferred method is to log on to the Support portal at support.broadcom.com . (You must initially register to gain access to the Support portal.) Once registered, log on and then select Hardware > Brocade Storage Networking . You can now navigate to any of the Brocade tools.	For Severity 1 (critical) issues, call Brocade Fibre Channel Networking Global Support at one of the phone numbers listed at www.broadcom.com/support/fibre-channel-networking/contact-brocade-support .

Document Feedback

Quality is our first concern. We have made every effort to ensure the accuracy and completeness of this document. However, if you find an error or an omission or if you think that a topic needs further development, we want to hear from you. Send your feedback to documentation.pdl@broadcom.com. Provide the publication title; topic heading; publication number and page number (for PDF documents); URL (for HTML documents); and as much detail as possible.

Overview of System Messages

This section summarizes the various types of system messages, their severity levels, log details, modules, configuration parameters, and so on.

System Message Types

Fabric OS supports three types of system messages. A system message can be one or more of the following types:

- Log Messages
- Audit Messages
- FFDC Messages

Fabric OS supports a different methodology for storing and accessing each type of message.

Log Messages

RASLog messages report significant information or system events (failures, errors, or critical conditions) and are also used to show the status of high-level, user-initiated actions. RASLog messages are forwarded to the console, to the configured syslog servers, and to the SNMP management station through Simple Network Management Protocol (SNMP) traps or informs.

The following is an example of a RASLog system message.

```
2021/10/12-17:51:05, [C4-1001], 937, SLOT 1 | CHASSIS, ERROR, switch, Port 18 failed due to SFP
validation failure. Check if the SFP is valid for the configuration.
```

For information on displaying and clearing RASLog messages, see [Displaying System Message Logs and Attributes](#).

NOTE

The *Recommended Action* field has been removed for messages that do not require any action from the user.

Audit Messages

Event auditing is designed to support post-event audits and problem determination based on high-frequency events of certain types such as security violations, zoning configuration changes, firmware downloads, and certain types of fabric events. Audit messages that are flagged only as AUDIT are not saved in the switch error logs. The switch can be configured to stream audit messages to the switch console and to forward the messages to specified syslog servers. Audit log messages are not forwarded to an SNMP management station. There is no limit to the number of audit events.

The following is an example of an audit message.

```
0 AUDIT, 2021/10/14-17:04:51 (GMT), [SULB-1003], 13627, SLOT 1 | CHASSIS, INFO, Ven60, Firmwarecommit
has started.
```

For any given event, audit messages capture the following information:

- User Name: The name of the user who triggered the action.
- User Role: The access level of the user, such as maintenance or admin.
- Event Name: The name of the event that occurred.
- Event Information: Information about the event.

The event classes described in the below table can be audited.

Table 1: Event Classes

Operand	Event Class	Description
1	Zone	You can audit zone event configuration changes, but not the actual values that were changed. For example, you may receive a message that states <code>Zone configuration has changed</code> , but the message does not display the actual values that were changed.
2	Security	You can audit any user-initiated security event for all management interfaces. For events that have an impact on the entire fabric, an audit is generated only for the switch from which the event was initiated.
3	Configuration	You can audit configuration downloads of existing SNMP configuration parameters. Configuration uploads are not audited.
4	Firmware	You can audit configuration downloads of existing SNMP configuration parameters. Configuration uploads are not audited.
5	Fabric	You can audit changes related to the Administration Domain.
7	LS	You can audit changes related to Virtual Fabrics (logical switches)
8	CLI	You can audit the CLI commands issued on the switch.
9	MAPS	You can audit changes related to Monitoring and Alerting Policy Suite (MAPS).
N/A	RAS	The RAS class is used to audit or track the RASLog messages or modules that are enabled or disabled using the <code>rasAdmin</code> command. The RAS class is not configurable, and it is always enabled internally.

Fabric OS v9.0.0 generates component-specific audit messages.

Event auditing is a configurable feature, that is enabled by default. You can also enable event auditing using the `auditCfg --enable` command to send events to a configured remote host. You can configure the system logging daemon (Syslogd) for logging/capturing audit messages. You can set up filters to screen out particular classes of events using the `auditCfg` command. The defined set of audit messages is sent to the configured remote host in the audit message format so that they are easily distinguishable from other syslog events that may occur in the network. For details on how to configure event auditing, see [Configuring Event Auditing](#). For more details, see [Displaying Audit Messages](#) and [Reading an Audit Message](#).

Audit Log Enhancements

The following audit logs have been enhanced or added for security events:

- Failure to establish an HTTPS connection along with the reason for the failure.
- Failure to establish an HTTPS connection if a peer presents an invalid certificate with an appropriate reason statement.
- Failure to establish an SSH session when a switch acts as a client (SSH/SCP/SFTP) including details of the reason for the failure and the remote IP to which the connection was attempted.
- Failure to establish an SSH session due to a cipher configuration mismatch or invalid ciphers when a switch acts as an SSH server including details of the reason for the failure and the remote IP to which the connection was attempted. (Use of ciphers that are not compliant with CC are discouraged but not enforced by the code. Hence, an SSH session will not fail if a valid cipher configuration is used, even though it is not compliant with CC.)
- Failure to establish an SSH session due to a supported public key algorithm mismatch or an invalid public key algorithm configuration when a switch acts as an SSH server including details of the reason for the failure and the remote IP to which the connection was attempted. (Use of public key algorithms that are not compliant with CC are

discouraged but not enforced by the code. Hence, an SSH session will not fail if a valid public key algorithm is used even though it is not compliant with CC.)

- Failure to establish an SSH session due to a supported MAC mismatch or an invalid MAC configuration when the switch acts as an SSH server including details of the reason for the failure and the remote IP to which the connection was attempted. (Uses of MAC that are not compliant with CC are discouraged but not enforced by the code. Hence, the SSH session will not fail if a valid MAC configuration is used even though it is not compliant with CC.)
- Failure to establish an SSH session due to a supported key exchange algorithm mismatch or an invalid key exchange algorithm configuration when switch acts as an SSH server including details of the reason for the failure and the remote IP to which the connection was attempted. (Use of key exchange algorithms that are not compliant with CC are discouraged but not enforced by code. Hence, the SSH session will not fail if a valid key exchange algorithm configuration is used even though it is not compliant with CC.)
- Failure to establish a TLS session due to a cipher configuration mismatch or invalid ciphers when the switch acts as a TLS client (RADIUS, LDAP, SYSLOG) including details of the reason for the failure. (Use of ciphers that are not compliant with CC are discouraged but not enforced by the code. Hence, the TLS session will not fail if a valid cipher configuration is used even though it is not compliant with CC.)
- Failure to establish a TLS connection when a switch acts as a TLS client (RADIUS, LDAP, SYSLOG) if a peer presents an invalid certificate with an appropriate reason statement.
- Failure to establish a TLS connection when a switch acts as a TLS client (RADIUS, LDAP, SYSLOG) due to a mutual authentication failure (using X509v3 certificates) with an appropriate reason statement.
- Failure to establish a TLS session due to a cipher configuration mismatch or invalid ciphers when a switch acts as a TLS server (HTTPS) including details of the reason for the failure. (Use of ciphers that are not compliant with CC are discouraged but not enforced by the code. Hence, the TLS session will not fail if a valid cipher configuration is used even though it is not compliant with CC.)
- Failure to establish a TLS session due to TLS protocol version configuration mismatch or an invalid TLS protocol version when a switch acts as a TLS server (HTTPS) including details of the reason for the failure. (Use of TLS

protocol versions that are not compliant with CC are discouraged but not enforced by the code. Hence, the TLS session will not fail if a valid cipher configuration is used even though it is not compliant with CC.)

- Failure to establish a TLS connection when a switch acts as a TLS server (HTTPS) due to a mutual authentication failure (using X509v3 certificates) with an appropriate reason statement.
- Failure to establish a TLS connection when a switch acts as a TLS server (HTTPS) if a peer presents an invalid certificate with an appropriate reason statement.
- Failure to establish a TLS connection when a switch acts as a TLS server (HTTPS) and the distinguished name (DN) or subject alternative name (SAN) of the peer does not match the expected identifier for the peer with an appropriate reason statement.
- Successful user authentication including details of the username, the interface used for login (SSH/Telnet/console/Web Tools), the remote IP address from which the user has connected, and the authentication mechanism used (RADIUS/LDAP/TACACS+/local).
- Failure to validate an X509v3 certificate including details of the reason for the failure.
- Failure to validate a CA certificate when the Basic Constraints extension is not present or when the CA flag is not set to true including details of the reason for the failure.
- Change of date on the switch.
- Query for the existing firmware version or the latest installed firmware version by the administrator.
- Firmware signature verification status (success or failure) before the firmware download process.
- Timeout expiry and session logout due to session inactivity of a remote interactive session (SSH/Telnet/Web Tools).
- Timeout expiry and session logout due to session inactivity of a local interactive session (console).
- User-initiated logout of session.
- Successful or failed attempt to establish a TLS client connection and to terminate an existing TLS session (SYSLOG) including details of the peer to which the connection was made.
- Successful or failed attempt to establish a TLS server connection or SSH connection and to terminate an existing TLS session (HTTPS) or SSH session including details of the peer to which the connection was made.
- If the certificate public key size is less than 2048 in the case of TLS, an event is audit-logged (although the connection is allowed).
- If certificate validation fails for the "Basic Constraints" field, an event is audit-logged and the connection is not allowed.
- If certificate validation fails for the "CN" (common name) field, an event is audit-logged and the connection is not allowed.
- If certificate validation fails for the "Extended Key Usage" field, an event is audit-logged and the connection is not allowed.

Audit Messages Related to SSH

The following are the audit messages related to SSH and these messages are used for:

- Key mismatch
- Cipher mismatch
- Key algorithm mismatch
- MAC mismatch Message template:

```
<Message Number="3076" Audit="YES" Log="YES" Class="SECURITY" Severity="INFO">
<Text>Event: %s, %s, Info: %s.</Text>
<Args>
<Arg>Event Name</Arg>
<Arg>Event action</Arg>
<Arg>Even specific info </Arg>
</Args>
<Cause>
```

<p>Indicates a failure to establish an SSH session.</p>

</Cause>

<Action>

<p>Verify the security event was planned.

If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy. </p>

</Action>

</Message>

Example message:

```
63 AUDIT, 2019/03/20-18:14:00 (UTC), [SEC-3076], INFO, SECURITY, NONE/NONE/NONE/None/CLI, None/sw0/ FID
128, , Event: SSH, Status: failed, Info: SSH Session establishment failed. Reason: no matching cipher found.,
IP Addr:10.70.12.112
```

Audit Messages Related to TLS

The following are the audit messages related to TLS and these messages are used for:

- Wrong protocol version
- Wrong ciphers
- Wrong CA certificate
- Server keys less than 2048

Message template:

<Message Number="3077" Audit="YES" Log="YES" Class="SECURITY" Severity="INFO">

<Text>Event: %s, %s, Info: %s.</Text>

<Args>

<Arg>Event Name</Arg>

<Arg>Event action</Arg>

<Arg>Even specific info </Arg>

</Args>

<Cause>

<p>Indicates a failure to establish a TLS session.</p>

</Cause>

<Action>

<p>Verify the security event was planned. If the security event was planned, no action is required.

If the security event was not planned, take appropriate action as defined by your enterprise security policy. </p>

</Action>

</Message>

Example message:

```
84 AUDIT, 2019/03/20-18:33:13 (UTC), [SEC-3077], INFO, SECURITY,
admin/admin/NONE/console/CLI, ad_0/sw0/FID 128, , Event: TLS SESSION, TLS handshake failed, Info: Wrong
Protocol version number..
```

Audit Messages Related to Certificate Validation

These messages are used for all types of certification validation failure: key usage, extended key usage, self-signed certificates, login with importing CA cert, CN mismatch and so on. Open SSL errors are presented in the info section as is.

Message template:

```
<Message Number="3081" Audit="YES" Log="YES" Class="SECURITY" Severity="INFO">
<Text>Event: %s, %s, Info: %s.</Text>
<Args>
<Arg>Event Name</Arg>
<Arg>Event action</Arg>
<Arg>Even specific info </Arg>
</Args>
<Cause>
<p>Indicates that TLS Certificate Validation failed.</p>
</Cause>
<Action>
<p>Verify the security event was planned.
If the security event was planned, no action is required.
If the security event was not planned, take appropriate action as defined by your enterprise security
policy. </p>
</Action>
</Message>
```

Example message:

```
94 AUDIT, 2019/03/20-18:37:04 (UTC), [SEC-3081], INFO, SECURITY,
swadmin/admin/10.252.200.228/ssh/CLI, ad_0/sw0/FID 128, , Event: TLS
SESSION, Certificate Validation failed, Info: Reason = unable to get local issuer certificate
Example messages for TLS initiation and termination:
INFO, pizzabox12,2019/04/13-12:19:45, [SEC-3078], 54908, FID 3, INFO, pizzabox12,
Event: TLS SESSION, TLS handshake, Info: Establishing TLS connection. Host=10.38.37.161. 2019/04/13-12:19:46,
[SEC-3078], 54909, FID 3,
Event: TLS SESSION, TLS handshake, Info: Terminating TLS connection. Host=10.38.37.161
```

Audit Messages Related to When Unsecure Protocols Are Allowed or Secure Protocols Are Disabled

The following are the audit messages that are related to unsecure and secure protocol usage. These messages are used in the following cases:

- When an ipfilter policy that has HTTP port (80) enabled is activated.
- When an ipfilter policy that has Telnet port (80) enabled is activated.
- When an ipfilter policy that has HTTPS port (443) disabled is activated. Message template:

```
<Message Number="3075" Audit="YES" Log="YES" Class="SECURITY" Severity="INFO">
<Text>Event: %s, %s, Info: %s.</Text>
<Args>
<Arg>Event Name</Arg>
```

```

<Arg>Event action</Arg>
<Arg>Even specific info </Arg>
</Args>
<Cause>
<p>Indicates that unsecure communication service is activated.</p>
</Cause>
<Action>
<p>Verify the security event was planned.
If the security event was planned, no action is required.
If the security event was not planned, take appropriate action as defined by your enterprise security
policy. </p>
</Action>
</Message>

```

Example messages for each of the above cases:

```

3 AUDIT, 2019/02/21-19:39:35 (UTC), [SEC-3075], INFO, SECURITY,
admin/admin/NONE/console/CLI, ad_0/sw0/FID 128, , Event: ipfilter,
HTTP PORT STATE: ACTIVE, Info: Activated ipfilter policy <policy_name> has activated HTTP port. 4 AUDIT,
2019/02/21-19:39:35 (UTC), [SEC-3075], INFO, SECURITY,
admin/admin/NONE/console/CLI, ad_0/sw0/FID 128, , Event: ipfilter,
TELNET PORT STATE: ACTIVE, Info: Activated ipfilter policy <policy_name> has activated Telnet port. 3 AUDIT,
2019/02/21-19:27:56 (UTC), [SEC-3075], INFO, SECURITY,
admin/admin/NONE/console/CLI, ad_0/sw0/FID 128, , Event: ipfilter,
HTTPS PORT STATE: DROP, Info: Activated ipfilter policy <policy_name> has blocked HTTPS port.

```

FFDC Messages

First Failure Data Capture (FFDC) is used to capture failure-specific data when a problem or failure is noted for the first time and before the switch reboots or the trace and log buffer is wrapped. All subsequent iterations of the same error are ignored. This critical debug information is saved in nonvolatile storage and can be retrieved using the `supportSave` command. The FFDC data is used for debugging or analyzing the problem. FFDC is intended for use by Brocade technical support.

FFDC is enabled by default. Enter the `supportFfdc` command to enable or disable FFDC. If FFDC is disabled, the FFDC daemon does not capture any data, even when a message with an FFDC attribute is logged.

The following is an example of an FFDC message.

```

2019/12/17-08:30:13, [SS-1000], 88, SLOT 6 | FFDC | CHASSIS, INFO, DCX, supportSave has uploaded support
information to the host with IP address 192.0.2.2.

```

Message Severity Levels

The Severity Levels of a Message table explains the four levels of severity for system messages, ranging from CRITICAL (1) to INFO (4). In general, the definitions are wide ranging and are to be used as general guidelines for troubleshooting. For all cases, you must look at each specific error message description thoroughly before taking action.

Table 2: Severity Levels of a Message

Severity Level	Description
1 = CRITICAL	Critical-level messages indicate that the software has detected serious problems that will cause a partial or complete failure of a subsystem if not corrected immediately; for example, a power supply failure or a rise in temperature must receive immediate attention.
2 = ERROR	Error-level messages represent an error condition that does not impact overall system functionality significantly. For example, error-level messages might indicate timeouts on certain operations, failures of certain operations after retries, invalid parameters, or failure to perform a requested operation.
3 = WARNING	Warning-level messages highlight a current operating condition that should be checked or it may lead to a failure in the future. For example, a power supply failure in a redundant system relays a warning that the system is no longer operating in redundant mode unless the failed power supply is replaced or fixed.
4 = INFO	Info-level messages report the current non-error status of the system components: for example, detecting the Online and off line status of a fabric port.

System Error Message Logging

The RASLog service generates and stores messages related to abnormal or erroneous system behavior. It includes the following features:

- All RASLog error messages are saved to nonvolatile storage by default.
- The system error message log can save a maximum of 8196 messages in random access memory (RAM).
- The system message log is implemented as a circular buffer. When more than the maximum entries are added to the log file, old entries are overwritten by new entries.
- Messages are numbered sequentially from 1 to 2,147,483,647 (0x7ffffff). The sequence number will continue to increase beyond the storage limit of 1024 messages. The sequence number can be reset to 1 using the `errClear` command. The sequence number persists across power cycles and switch reboots.
- The RASLog message text can be up to 256 characters long.
- Trace dump, FFDC, and core dump files can be uploaded to the FTP server using the `supportSave` command.
- Configure the syslogd facility as a management tool for error logs. This is particularly important for dual-domain switches because the syslogd facility saves messages from two logical switches as a single file and in sequential order. For more information, see [System Logging Daemon](#).
- RASLog messages are streamed to the console and are forwarded to the configured syslog servers and to the SNMP management station through SNMP traps (in SNMPv1 and SNMPv3) or through informs (in SNMPv3). Use the `snmpConfig` command to configure the SNMPv1 and SNMPv3 hosts.
- Audit messages are streamed to the switch console and are forwarded to the configured syslog servers. The audit log messages are not forwarded to an SNMP management station.

Configuring Syslog Message Destinations

You can configure Fabric OS to send syslog messages to the following output locations:

- Syslog daemon
- System console
- SNMP management station

System Logging Daemon

The system logging daemon (syslogd) is a process on UNIX, Linux, and some Windows systems that reads and logs messages as specified by the system administrator.

Fabric OS can be configured to use a UNIX-style syslogd process to forward system events and error messages to log files on a remote host system. The host system can be running UNIX, Linux, or any other operating system that supports

standard syslogd functionality. Configuring syslogd involves configuring the host, enabling syslogd on the Brocade model, and optionally setting the facility level.

Configuring a Syslog Server

To configure the switch to forward all system events and error messages to the syslogd of one or more servers, perform the following steps.

1. Log in to the switch as admin.
2. Use the `syslogadmin --set -ip ip_address | hostname [-port port_num]` command to configure a secure and nonsecure syslog server to which system messages are forwarded. Secure syslog mode is disabled by default.

The following example configures an IPv4 nonsecure syslog server:

```
switch:admin> syslogadmin --set -ip 172.26.26.173
```

The following example configures an IPv4 secure syslog server:

```
switch:admin> syslogadmin --set -ip 172.26.26.173 -secure -port 2000
```

The following example configures a nonsecure syslog server using a hostname. `switch:admin> syslogadmin --set -ip win2k8-58-113`

You can configure up to six syslog servers to receive syslog messages.

3. Enter the `syslogadmin --show -ip` command to verify the syslog configuration on the switch.

```
switch:admin> syslogadmin --show -ip
syslog.1 172.26.26.173
syslog.2 win2k8-58-113
```

You can remove a configured syslog server using the `syslogadmin --remove -ip ip_address | hostname` command.

System Console

The system console displays RASLog messages, audit messages (if enabled), and panic dump messages. These messages are mirrored to the system console in addition to being saved in one of the system logs.

The system console displays messages only through the serial port. If you log in to a switch through the Ethernet port or modem port, you will not receive system console messages.

You can filter messages that display on the system console by severity using the `errFilterSet` command. All messages are still sent to the system message log and syslogd (if configured).

Setting the System Console Severity Level

You can limit the types of messages that are logged to the console using the `errFilterSet` command. This command allows you to set the minimum severity level to be logged to the console. All error messages at that level or higher will be logged; all error messages below that level will not be displayed, but they will still be recorded. You can choose one of the following severity levels: INFO, WARNING, ERROR, or CRITICAL.

To set the severity levels for the system console, perform the following steps.

1. Log in to the switch as admin.
2. Use the `errFilterSet [-d console -v severity]` command to set the console severity level. The *severity* can be one of the following: INFO, WARNING, ERROR, or CRITICAL. The *severity* values are not case-sensitive.

For example, to set the filter severity level for the console to ERROR, enter the following command.

```
switch:admin> errfilterset -d console -v error
```

3. Enter the `errFilterSet` command to verify the configured filter settings.

```
switch:admin> errfilterset
```

```
console: filter severity = ERROR
```

SNMP Trap Recipient

An unsolicited message that comes to the management station from the SNMP agent on the device is called a *trap*. When an event occurs and if the event severity level is at or below the set severity level, the SNMP trap notification, `swEventTrap`, is sent to the configured trap recipients. The `VarBind` in the Trap Data Unit contains the corresponding instance of the event index, time information, event severity level, repeat count, and description. The following severity levels are possible:

- None (0)
- Critical (1)
- Error (2)
- Warning (3)
- Informational (4)
- Debug (5)

By default, the severity level is set to None, implying that all traps are filtered and therefore no event traps are received. When the severity level is set to Informational, all traps with the severity level of Informational, Warning, Error, and Critical are received. For more information on changing the severity level of `swEvent` Audit messages are not converted into `swEventTrap`.

SNMP traps are unreliable because the trap recipient does not send any acknowledgment when it receives a trap. Therefore, the SNMP agent cannot determine if the trap was received.

Brocade switches send traps on UDP port 162. To receive traps, the management station IP address must be configured on the switch. You can configure SNMPv1 and SNMPv3 hosts to receive traps.

For more information on the `swEventTrap`, refer to the *Brocade® Fabric OS® MIB Reference Manual*.

Configuring the SNMPv1 Trap Recipient

The `snmpConfig --set snmpv1` command allows you to specify the SNMP trap recipient. To configure the SNMPv1 host to receive the trap, perform the following steps:

1. Log in to the switch as admin.
2. Enter the `snmpConfig --set snmpv1` command to configure the SNMP trap recipient.

```
switch:admin> snmpconfig --set snmpv1
SNMP community and trap recipient configuration:
Community (rw): [Secret C0de]
Trap Recipient's IP address : [192.0.2.2]
Trap recipient Severity level : (0..5) [4]
Trap recipient Port : (0..65535) [162]
Community (rw): [OrigEquipMfr]
Trap Recipient's IP address : [fec0:60:22bc:200:313:72ff:fe64:78b2]
```

NOTE

To receive the traps, the management station IP address must be configured on the switch.

3. Enter the `snmpConfig --show snmpv1` command to verify the SNMPv1 agent configuration.

```
switch:admin> snmpconfig --show snmpv1
SNMPv1 community and trap recipient configuration: Community 1: Secret C0de (rw)
Trap recipient: 192.0.2.2
Trap port: 162
```



```

Trap recipient Severity level: 5 Community 2: OrigEquipMfr (rw)
Trap recipient: fec0:60:22bc:200:313:72ff:fe64:78b2 Trap port: 162
Trap recipient Severity level: 5 Community 3: private (rw)
Trap recipient: tools.lab.brocade.com Trap port: 162
Trap recipient Severity level: 5 Community 4: public (ro)
Trap recipient: 192.0.10.10
Trap port: 65530
Trap recipient Severity level: 1 Community 5: common (ro)
Trap recipient: fec0:60:69bc:200:213:72ff:fe64:069f Trap port: 11
Trap recipient Severity level: 2 Community 6: FibreChannel (ro)
Trap recipient: WT.org.brocade.com Trap port: 65521
Trap recipient Severity level: 2 SNMPv1:Enabled

```

Configuring the SNMPv3 Trap Recipient

To configure the SNMPv3 host to receive traps, perform the following steps:

1. Log in to the switch as admin.
2. Enter the `snmpConfig --set snmpv3` command to configure the SNMP trap recipient. Ignore the step to enable the SNMP informs: **SNMP Informs Enabled**.

```

switch:admin> snmpconfig --set snmpv3
SNMP Informs Enabled (true, t, false, f): [false] t
SNMPV3 Password Encryption Enabled (true, t, false, f): [false] t
Warning: The encrypted password cannot be decrypted. Do you want to continue? (yes, y, no, n): [no] y
SNMPv3 user configuration(snmp user not configured in FOS user database will have default VF context and
  admin role as the default):
User (rw): [snmp_auto_v3]
Auth Protocol [MD5(1)/SHA(2)/noAuth(3)]: (1..3) [3]
Priv Protocol [DES(1)/noPriv(2)/AES128(3)/AES256(4)]: (2..2) [2]
Engine ID: [00:00:00:00:00:00:00:00:00]
User (rw): [snmp_auto_v10_10]
Auth Protocol [MD5(1)/SHA(2)/noAuth(3)]: (1..3) [1] New Auth Passwd:
Priv Protocol [DES(1)/noPriv(2)/AES128(3)/AES256(4)]: (1..4) [1]
New Priv Passwd:
Engine ID: [00:00:00:00:00:00:00:00:00]
User (rw): [snmp_auto_v128_12]
Auth Protocol [MD5(1)/SHA(2)/noAuth(3)]: (1..3) [1] New Auth Passwd:
Priv Protocol [DES(1)/noPriv(2)/AES128(3)/AES256(4)]: (1..4) [1]
New Priv Passwd:
Engine ID: [00:00:00:00:00:00:00:00:00]
SNMPv3 trap/inform recipient configuration:
Trap Recipient's IP address : [0.0.0.0] 192.168.10.10
Notify Type [TRAP(1)/INFORM(2)]: (1..2) [1] 1
UserIndex: (1..12) [1] 10
Trap recipient Severity level : (0..5) [0] 5
Trap recipient Port : (0..65535) [162]
Trap Recipient's IP address : [0.0.0.0] 10.10.10.10

```

```

Notify Type [TRAP(1)/INFORM(2)]: (1..2) [1]
UserIndex: (1..12) [2] 12
Trap recipient Severity level : (0..5) [0] 4
Trap recipient Port : (0..65535) [162] Trap Recipient's IP address : [0.0.0.0] Trap Recipient's IP
address : [0.0.0.0] Trap Recipient's IP address : [0.0.0.0] Trap Recipient's IP address : [0.0.0.0]
Committing configurationdone.

```

NOTE

To receive the SNMP traps, the username, the authentication protocol, the UDP port number, and the privacy protocol must match between the switch and the management station.

3. Enter the `snmpConfig --show snmpv3` command to verify the SNMP agent configuration.

```

switch:admin> snmpconfig --show snmpv3
SNMP Informs = 1 (ON)
SNMPV3 user password encrypted = 1 (ON) SNMPv3 USM configuration:
User 1 (rw): snmp_auto_v3 Auth Protocol: noAuth Priv Protocol: noPriv
Engine ID: 80:90:00:00:00:00:00:ab
User 2:
User 3:
User 4:
User 5:
User 6:
User 7:
User 8:
User 9:
User 10 (rw): snmp_auto_v10_10 Auth Protocol: MD5
Priv Protocol: DES
Engine ID: 00:00:00:00:00:00:00:00
User 11:
User 12 (rw): snmp_auto_v128_12 Auth Protocol: MD5
Priv Protocol: DES
Engine ID: 00:00:00:00:00:00:00:00
SNMPv3 Trap/Informs configuration:
Trap Entry 1: 192.168.10.10
Trap Port: 162
Trap User: snmp_auto_v3
Trap recipient Severity level: 5 Notify Type: TRAP(1)
Trap Entry 2: 10.10.10.10
Trap Port: 162
Trap User: snmp_auto_v128_12 Trap recipient Severity level: 4 Notify Type: TRAP(1)
Trap Entry 3: No trap recipient configured yet Notify Type: TRAP(1)
Trap Entry 4: No trap recipient configured yet Notify Type: TRAP(1)
Trap Entry 5: No trap recipient configured yet Notify Type: TRAP(1)
Trap Entry 6: No trap recipient configured yet Notify Type: TRAP(1)

```

SNMP Inform Recipient

The SNMP inform notification is similar to the SNMP trap except that the management station that receives an SNMP inform acknowledges the system message with an SNMP response packet data unit (PDU). If the sender does not receive the SNMP response PDU, the inform request can be sent again. An SNMP inform request is saved in the switch memory until a response is received or the request times out. Informers are more reliable than traps, but they consume more resources in the device and in the network. Use SNMP informers only if it is important that the management station receives all event notifications. Otherwise, use SNMP traps.

Configuring the SNMPv3 Inform Recipient

To configure an SNMPv3 host to receive SNMP informers, perform the following steps:

1. Log in to the switch as admin.
2. Enter the `snmpConfig--set snmpv3` command to configure the inform recipient. When prompted to enable the SNMP informers, enter `true` or `t`. SNMP informers are disabled by default.

```
switch:admin> snmpconfig --set snmpv3
SNMP Informers Enabled (true, t, false, f): [true]
SNMPV3 Password Encryption Enabled (true, t, false, f): [true]
SNMPv3 user configuration(snmp user not configured in FOS user database will have default VF context and
admin role as the default):
User (rw): [snmp_auto_v3]
Auth Protocol [MD5(1)/SHA(2)/noAuth(3)]: (1..3) [3]
Priv Protocol [DES(1)/noPriv(2)/AES128(3)/AES256(4)]: (2..2) [2] Engine ID: [00:00:00:00:00:00:00:00]
80:90:00:00:00:00:00:AB
User (rw): [snmp_auto_v10_10]
Auth Protocol [MD5(1)/SHA(2)/noAuth(3)]: (1..3) [1] New Auth Passwd:
Priv Protocol [DES(1)/noPriv(2)/AES128(3)/AES256(4)]: (1..4) [1]
New Priv Passwd:
Engine ID: [00:00:00:00:00:00:00:00]
User (rw): [snmp_auto_v128_12]
Auth Protocol [MD5(1)/SHA(2)/noAuth(3)]: (1..3) [1]
New Auth Passwd:
Priv Protocol [DES(1)/noPriv(2)/AES128(3)/AES256(4)]: (1..4) [1]
New Priv Passwd:
Engine ID: [00:00:00:00:00:00:00:00]
SNMPv3 trap/inform recipient configuration:
Trap Recipient's IP address : [192.168.10.10] Notify Type [TRAP(1)/INFORM(2)]: (1..2) [1] 2
UserIndex: (1..12) [10] 1
Trap recipient Severity level : (0..5) [5] Trap recipient Port : (0..65535) [162]
Trap Recipient's IP address : [10.10.10.10] Notify Type [TRAP(1)/INFORM(2)]: (1..2) [1]
UserIndex: (1..12) [12]
Trap recipient Severity level : (0..5) [4] Trap recipient Port : (0..65535) [162] Trap Recipient's IP
address : [0.0.0.0] Trap Recipient's IP address : [0.0.0.0] Trap Recipient's IP address : [0.0.0.0] Trap
Recipient's IP address : [0.0.0.0] Committing configurationdone.
```

NOTE

To receive the SNMP informers, the username, the authentication protocol, the privacy protocol, the UDP port number, and the engine ID must match between the switch and the management station.

3. Enter the `snmpConfig --show snmpv3` command to verify the SNMP agent configuration.

```
switch:admin> snmpconfig --show snmpv3
SNMP Informs = 1 (ON)
SNMPV3 user password encrypted = 1 (ON) SNMPv3 USM configuration:
User 1 (rw): snmp_auto_v3 Auth Protocol: noAuth Priv Protocol: noPriv
Engine ID: 80:90:00:00:00:00:00:ab
User 2:
User 3:
User 4:
User 5:
User 6:
User 7:
User 8:
User 9:
User 10 (rw): snmp_auto_v10_10 Auth Protocol: MD5
Priv Protocol: DES
Engine ID: 00:00:00:00:00:00:00:00
User 11:
User 12 (rw): snmp_auto_v128_12 Auth Protocol: MD5
Priv Protocol: DES
Engine ID: 00:00:00:00:00:00:00:00
SNMPv3 Trap/Informs configuration: Trap Entry 1: 192.168.10.10
Trap Port: 162
Trap User: snmp_auto_v3
Trap recipient Severity level: 5 Notify Type: INFORM(2)
Trap Entry 2: 10.10.10.10
Trap Port: 162
Trap User: snmp_auto_v128_12 Trap recipient Severity level: 4 Notify Type: TRAP(1)
Trap Entry 3: No trap recipient configured yet Notify Type: TRAP(1)
Trap Entry 4: No trap recipient configured yet Notify Type: TRAP(1)
Trap Entry 5: No trap recipient configured yet Notify Type: TRAP(1)
Trap Entry 6: No trap recipient configured yet Notify Type: TRAP(1)
```

Port Logs

Fabric OS maintains an internal log of all port activity, with each switch or logical switch maintaining a log file for each port. Port logs are circular buffers that can save up to 8000 entries per logical switch. When the log is full, the newest log entries automatically overwrite the oldest log entries. Port logs capture switch-to-device, device-to-switch, switch-to-switch, some device-A-to-device-B, and control information. Port logs are not persistent and are lost over power cycles and reboots. Port log functionality is completely separate from the system message log. Port logs are typically used to troubleshoot device connections.

To display the port logs for a particular port, enter the `portLogShow` command.

To display the specific events logged for each port, enter the `portLogEventShow` command.

Changing the swEventTrap Severity Level

When an event occurs and the event severity level is at or below the set severity level, the SNMP event trap notification, swEventTrap, is sent to the configured trap recipients. By default, the severity level is set at 0 (None), resulting in all event traps being sent. Use the snmpConfig --set mibCapability command to modify the severity level of swEventTrap.

To change the severity level of swEventTrap, perform the following steps:

1. Log in to the switch as admin.
2. Enter the snmpConfig --set mibCapability command to configure MIBs interactively. All supported MIBs and associated traps are displayed. You can change the desired severity for swEventTrap to 1 (Critical), 2 (Error), 3 (Warning), or 4 (Informational). The default value is 0.

```
switch:admin> snmpconfig --set mibcapability
FE-MIB: YES SW-MIB: YES FA-MIB: YES
FICON-MIB: YES HA-MIB: YES FCIP-MIB: YES ISCSI-MIB: YES IF-MIB: YES
BD-MIB: YES SW-TRAP: YES
swFault: YES swSensorScn: YES
swFCPortScn: YES swEventTrap: YES
DesiredSeverity:Informational
swFabricWatchTrap: YES
DesiredSeverity:None swTrackChangesTrap: YES swIPv6ChangeTrap: YES swPmgrEventTrap: YES
swFabricReconfigTrap: YES swFabricSegmentTrap: YES
swExtTrap: NO swStateChangeTrap: NO swPortMoveTrap: NO swBrcdGenericTrap: YES
... <lines omitted for brevity> SW-TRAP (yes, y, no, n): [yes]
swFault (yes, y, no, n): [yes] swSensorScn (yes, y, no, n): [yes] swFCPortScn (yes, y, no, n): [yes]
swEventTrap
(yes,
y,
no,
n):
[yes]
DesiredSeverity:
(0..4)
[4]
3
swFabricWatchTrap (yes, y, no, n): [yes]
DesiredSeverity: (0..4) [0] 2 swTrackChangesTrap (yes, y, no, n): [yes] swIPv6ChangeTrap (yes, y, no, n):
[yes] swPmgrEventTrap (yes, y, no, n): [yes]
[...]
```

3. Enter the snmpConfig --show mibCapability command to verify the severity level of swEventTrap.

```
switch:admin> snmpconfig
--show
mibcapability
FE-MIB: YES SW-MIB: YES FA-MIB: YES
FICON-MIB: YES HA-MIB: YES FCIP-MIB: YES ISCSI-MIB: YES IF-MIB: YES
BD-MIB: YES SW-TRAP: YES
swFault: YES swSensorScn: YES swFCPortScn: YES
swEventTrap:
YES
```

DesiredSeverity:Informational

swFabricWatchTrap: YES

DesiredSeverity:Critical swTrackChangesTrap: YES swIPv6ChangeTrap: YES

swPmgrEventTrap: YES swFabricReconfigTrap: YES

[...]

Commands for Displaying and Configuring System Message Logs

The Commands for Viewing or Configuring System Parameters and Message Logs table describes commands that you can use to view or configure the system message logs. Most commands require admin-level access privileges. For detailed information on required access levels and commands, refer to the *Brocade® Fabric OS® Command Reference Manual*.

Table 3: Commands for Viewing or Configuring System Parameters and Message Logs

Command	Description
auditCfg	Configures the audit message log.
auditDump	Displays or clears the audit log.
errClear	Clears all error log messages for all switch instances on this control processor (CP).
errDelimiterSet	Sets the error log start and end delimiter for messages pushed to the console.
errDump	Displays the entire error log, without page breaks. Use the -r option to show the messages in reverse order, from newest to oldest.
errFilterSet	Sets an error severity filter for the system console.
errModuleShow	Displays all defined error log modules.
errShow	Displays the entire error log, with page breaks. Use the -r option to show the messages in reverse order, from newest to oldest.
pdShow	Displays the contents of the panic dump and core dump files.
portErrShow	Displays the port error summary.
portLogClear	Clears the port log. If the port log is disabled, this command enables it.
portLogDisable	Disables the port log facility.
portLogDump	Displays the port log, without page breaks.
portLogDumpPort	Displays the port log of the specified port, without page breaks.
portLogEnable	Enables the port log facility.
portLogEventShow	Displays which port log events are currently being reported.
portLoginShow	Displays port logins.
portLogPdisc	Sets or clears the debug pdisc_flag.
portLogReset	Enables the port log facility.
portLogResize	Resizes the port log to the specified number of entries.
portLogShow	Displays the port log, with page breaks.
portLogShowPort	Displays the port log of the specified port, with page breaks.
portLogTypeDisable	Prevents an event from being reported in the port log. Port log events are described by the portLogEventShow command.
portLogTypeEnable	Configures an event to be reported in the port log. Port log events are described by the portLogEventShow command.

rasAdmin	Used to enable or disable logging for selected messages or modules, to change the default severity level for a specified message, to display configured RASLog message settings, and to enable or disable quiet time.
rasMan	Displays message documentation on the switch.
setVerbose	Sets the verbose level of a particular module within the Fabric OS.

Table 4: Commands for Viewing or Configuring System Parameters and Message Logs

Command	Description
snmpConfig	Manages the SNMP agent configuration.
supportFfdc	Enables and disables FFDC.
supportFtp	Sets, clears, or displays support FTP parameters or a time interval to check the FTP server.
supportSave	Collects RASLog, trace files, and supportShow (active CP only) information for the local CP and then transfers the files to an FTP server. The operation can take several minutes.
supportShow	Issues a list of diagnostic and error display commands. This output is used by your switch service provider to diagnose and correct problems with the switch. The output from this command is very long. Refer to the following related commands: supportShowCfgShow —Displays the groups of commands enabled for display by the supportShow command. supportShowCfgEnable —Enables a group of commands to be displayed under the supportShow command. supportShowCfgDisable —Disables a group of commands under the supportShow command.
syslogadmin --set - facility	Changes the syslogd facility.
syslogadmin --set - ip	Adds an IP address as a recipient of system messages.
syslogadmin --remove - ip	Removes an IP address as a recipient of system messages.
syslogadmin --show - ip	Displays the currently configured IP addresses that are recipients of system messages.
traceDump	Displays, initiates, or removes a Fabric OS module trace dump.

Displaying Message Content on the Switch

You can view the message documentation such as the message text, message type, class (for audit messages), message severity, cause, and action on the switch console by using the rasMan message_ID command.

To display the message documentation on the switch, perform the following steps:

1. Log in to the switch as admin.
2. Use the `rasMan message_ID` command to display the message documentation. The message_ID values are case-sensitive.

The following example displays the documentation for the PS-1007 message.

```
switch:admin> rasman PS-1007
Log Messages
PS-1007 (7m)
MESSAGE
```

PS-1007 - Failed to addFabricmodeTopTalker on domain=<domain id>. <function name>.

MESSAGE TYPE

LOG

SEVERITY

WARNING

PROBABLE CAUSE

Indicates that FC Routing (FCR) is enabled on the specified fabric.

RECOMMENDED ACTION

Top Talker cannot be installed on a fabric with FCR service enabled. In case Top Talker must be installed on a fabric, disable FCR using the `fosconfig --disable fcr` command.

Configuring System Messages and Attributes

This section provides information on configuring the system message logs and attributes. All admin-level commands mentioned in this section are used to enable or disable only the external messages.

Configuring Event Auditing

To configure event auditing, perform the following steps:

1. Log in to the switch as admin.
2. Enter the `auditCfg --enable` command to enable the audit feature.
3. Enter the `auditCfg --class` command to configure the event classes that you want to audit.

```
switch:admin> auditcfg --enable
```

Audit filter is enabled.

```
switch:admin> auditcfg --class 1,2,3,4,5,6,7,8,9
```

Audit filter is configured.

NOTE

The RAS audit class is not configurable, and it is always enabled internally.

4. Use the `auditCfg --severity severity-level` command to set the audit severity level. By default, all messages are logged. When the severity is set, only messages with the configured severity and higher are displayed. Valid values for *severity-level* are INFO, WARNING, ERROR, and CRITICAL.

```
switch:admin> auditcfg --severity ERROR
```

5. Enter the `auditCfg --show` command to verify the configuration.

```
switch:admin> auditcfg --show
```

Audit filter is enabled. 1-ZONE

SECURITY

CONFIGURATION

FIRMWARE

FABRIC

LS

CLI

MAPS

Severity level: ERROR

You must configure the syslog daemon to send audit events to a configured remote host using the `syslogdIpAdd` command. For more information on configuring the syslog server, see [Configuring a Syslog Server](#).

Disabling a RASLog Message or Module

To disable a single RASLog message or all messages in a module, perform the following steps:

1. Log in to the switch as admin.
2. Use the following commands to disable a single RASLog message or all messages that belong to a module:
 - The `rasadmin --show -log message_ID` command disables a RASLog message. The following example disables the BL-1001 message.


```
switch:admin> rasadmin --disable -log BL-1001
```

2017/07/20-13:30:41, [LOG-1005], 378, SLOT 4 | CHASSIS, INFO, switch, Log message NS-1009 has been disabled.

Use the `rasadmin --show -log message_ID` command to verify the status of the message.
 - The `rasadmin --disable -module module_ID` command disables all messages in a module. The following example disables all messages that belong to the BL module.


```
switch:admin> rasadmin --disable -module BL
```

2017/07/20-13:28:37, [LOG-1007], 375, SLOT 4 | CHASSIS, INFO, switch, Log Module BL has been disabled.
 - Use the `rasadmin --show -module module_ID` command to verify the status of the messages that belong to a module.

NOTE

You cannot disable audit and FFDC messages using the `rasadmin` command.

Enabling a RASLog Message or Module

To enable a single RASLog message or all messages in a module that were previously disabled, perform the following steps:

1. Log in to the switch as admin.
2. Use the following commands to enable a single RASLog message or all messages that belong to a module:
 - The `rasadmin --enable -log message_ID` command enables a single RASLog message that has been disabled.
 - The following example enables the BL-1001 message, which was previously disabled.


```
switch:admin> rasadmin --enable -log BL-1001
```

2017/10/15-13:24:30, [LOG-1006], 373, SLOT 4 | CHASSIS, INFO, switch, Log message BL-1001 has been enabled. Use the `rasadmin --show -log message_ID` command to verify the status of the message.
 - The `rasadmin --enable -module module_ID` command enables all messages in a module. The following example enables all previously disabled BL messages.


```
switch:admin> rasadmin --enable -module BL
```

2017/10/15-13:28:37, [LOG-1007], 375, SLOT 4 | CHASSIS, INFO, switch, Log Module BL has been enabled.
 - Use the `rasadmin --show -module module_ID` command to verify the status of the messages that belong to a module.

Setting the Severity Level of a RASLog Message

To change the default severity level of a RASLog message, perform the following steps:

1. Log in to the switch as admin.

2. Use the `rasadmin --set -log message_ID -severity [DEFAULT | INFO | WARNING | ERROR | CRITICAL]` command to change the severity level of a message. The following example changes the severity level of the C4-1004 message to WARNING.

```
switch:admin> rasadmin --set -log C4-1004 -severity WARNING
```

3. Use the `rasadmin --show -severity message_ID` command to verify the severity level of the message.

```
switch:admin> rasadmin --show -severity C4-1004
```

```
MessageSeverity C4-1004 :WARNING
```

Enabling Quiet Time for a Specified Message Type

To enable quiet time for a specified message type, perform the following steps:

1. Log in to the switch as admin.
2. Use the `rasadmin --quiet -enable log_type [-stime HH:MM] [-etime HH:MM] [-dow day_of_week]` command to enable quiet time for the specified message type.

The following example enables quiet time for audit messages for a duration of forever.

```
switch:admin> rasadmin --quiet -enable 1
```

The following example enables quiet time for audit messages at 22:00 daily and turns it off the next day at 02:00.

```
switch:admin> rasadmin --quiet -enable 1 -stime 22:00 -etime 02:00
```

The following example enables quiet time for RASLog messages on Monday and Wednesday at 07:00 and turns off at 12:00.

```
switch:admin> rasadmin --quiet -enable 2 -stime 07:00 -etime 12:00 -dow 1,3
```

The following example enables quiet time for both audit and RASlog messages for a duration of forever.

```
switch:admin> rasadmin --quiet -enable 3
```

Disabling Quiet Time for a Specified Message Type

To disable quiet time for a specified message type, perform the following steps:

1. Log in to the switch as admin.
2. Use the `rasadmin --quiet -disable log_type` command to disable quiet time for the specified message type. The following example disables quiet time for audit messages.

```
switch:admin> rasadmin --quiet -disable 1
```

Displaying System Message Logs and Attributes

This section provides information on displaying system message logs. These procedures are valid for all supported platforms.

Displaying RASLog Messages

To display the system message log on a switch with no page breaks, perform the following steps. You can display the messages in reverse order using the reverse option. To display message logs in all switches (logical switches), use the all option.

1. Log in to the switch as admin.
2. Enter the `errDump` command.

```
switch:admin> errdump
```

```

Version: 9.0.0
2020/12/17-05:54:30, [HAM-1004], 1, CHASSIS, INFO, switch, Processor rebooted - Reset
2020/12/17-05:55:04, [ZONE-1034], 2, FID 128, INFO, switch, A new zone database file is created.
2017/12/17-05:55:04, [FCR-1069], 3, FID 128, INFO, switch, The FC Routing service is enabled.
2020/12/17-05:55:04, [FCR-1068], 4, FID 128, INFO, switch, The FC Routing service is disabled.
2020/12/17-05:55:11, [EM-1034], 5, CHASSIS, ERROR, switch, PS 2 set to faulty, rc=2000e. [...]

```

Displaying RASLog Messages One Message at a Time

To display the system message log one message at a time, perform the following steps:

- Log in to the switch as admin.

```

Enter the errShow command. switch:admin> errShow Version: 9.0.0
2020/02/07-18:28:33, [SULB-1044], 3, CHASSIS, INFO, switch, Firmwaredownload to secondary partition has
completed successfully.
Type <CR> to continue, Q<CR> to stop:
2020/02/07-18:28:36, [FSSM-1002], 4, CHASSIS, INFO, switch, HA State is in sync.
Type <CR> to continue, Q<CR> to stop:
2020/02/07-18:28:39, [RAS-1007], 6, CHASSIS, INFO, switch, System is about to reload. Type <CR> to continue,
Q<CR> to stop:
[...]

```

Displaying Audit Messages

To display the audit messages, perform the following steps. The RAS-3005 message is generated for each CLI command issued on the switch and is saved in the audit message log.

1. Log in to the switch as admin.
2. Enter the `uditDump -s` command.

```

switch:admin> auditdump -s
AUDIT, 2018/02/22-10:58:01 (UTC), [MAPS-1020], WARNING, MAPS, NONE/admin/NONE/None/CLI, ad_0/
switch/FID 128, , Switch wide status has changed from HEALTHY to CRITICAL.
AUDIT, 2018/02/22-11:00:00 (UTC), [SULB-1004], INFO, FIRMWARE, NONE/admin/NONE/None/CLI, ad_0/
switch/CHASSIS, , Firmwarecommit has completed.
AUDIT, 2018/02/22-11:00:00 (UTC), [SULB-1002], INFO, FIRMWARE, NONE/admin/NONE/None/CLI, ad_0/
switch/CHASSIS, , Firmwaredownload command has completed successfully.
AUDIT, 2018/02/22-11:02:00 (UTC), [PORT-1008], INFO, CONFIGURATION, NONE/admin/NONE/None/CLI,
ad_0/switch/FID 128, , GigE Port (ID: 0) has been enabled.
AUDIT, 2018/02/22-11:06:29 (UTC), [SULB-1055], WARNING, FIRMWARE, NONE/admin/NONE/None/CLI,
ad_0/switch/FID 128, , Firmware upgrade on the blade in slot 0 has completed [...]

```

Displaying FFDC Messages

To show which messages will create the FFDC files, perform the following steps:

1. Log in to the switch as admin.

```

Enter the errDump --attribute FFDC command. switch:admin> errDump --attribute FFDC Fabric OS: 9.0.0
2020/10/15-10:39:02, [LOG-1002], 4496, SLOT 5 |FFDC, WARNING, switch, A log

```

message was not recorded.

2020/10/15-10:39:18, [RAS-1001], 4496, SLOT 5 |FFDC, WARNING, switch, First failure data capture (FFDC) event occurred. [...]

NOTE

See the supportSave output for details of the FFDC files that were saved.

Displaying the Status of System Messages

To display the status of system messages, perform the following steps:

1. Log in to the switch as admin.
2. Use the following commands to display the status of all messages in the log, the status of a specific message, or the status of all messages belonging to a module:
 - Enter the `rasadmin --show -all` command to display the status of all RASLog messages in the system log.


```
switch:admin> rasadmin --show -all
```

Message	Status	Default Severity	Current Severity
FCIP-1000	ENABLED	CRITICAL	CRITICAL
FCIP-1001	ENABLED	INFO	ERROR
FCIP-1002	ENABLED	INFO	INFO

[...]
 - Use the `rasadmin --show -log message_ID` command to display the status of a specified RASLog message.


```
switch:admin> rasadmin --show -log IPAD-1002
```

Message	Status	Default Severity	Current Severity
IPAD-1002	DISABLED	INFO	INFO
 - Use the `rasadmin --show -module module_ID` command to display the status of all messages belonging to a specified module.


```
switch:admin> rasadmin --show -module ECC
```

Message	Status	Default Severity	Current Severity
ECC-1000	ENABLED	ERROR	ERROR
ECC-1001	DISABLED	ERROR	WARNING
 - Use the `rasadmin --show -disabled` command to list all disabled RASLog messages.


```
switch:admin> rasadmin --show -disabled
```

Message	Status

Displaying the Severity Level of RASLog Messages

To display the severity level of a RASLog message, perform the following steps:

1. Log in to the switch as admin.
2. Use the `rasadmin --show -severity message_ID` command to display the severity level of a RASLog message. The following example displays the status of the PS-1007 message.


```
switch:admin> rasadmin --show -severity PS-1007
```

MessageSeverity PS-1007:WARNING

Displaying the Configured Quiet Time

To display the configured quiet time, perform the following steps:

1. Log in to the switch as admin.
2. Use the `rasadmin --quiet -show` command to display the configured quiet time.

```
switch:admin> rasadmin --quiet -show
Type      QuietTime  StartTime  EndTime    DayOfWeek
-----
AUDIT     ON           22:00      02:00      EVERYDAY
RASLOG    OFF          07:00      12:00      MON, WED
```

Displaying RASLog Messages by Severity Level

To display RASLog messages based on the severity level, perform the following steps:

1. Log in to the switch as admin.
2. Use the `errdump --severity [DEFAULT | INFO | WARNING | ERROR | CRITICAL]` command. For more information on message severity levels, see [Message Severity Levels](#). You can set the number of messages to display using the `count` option. The following example filters messages by the severity level of INFO.

```
switch:admin> errdump --count 4 --severity INFO
Fabric OS: 9.0.0
2020/10/07-18:19:47, [LOG-1003], 1, SLOT 5 |CHASSIS, INFO, switch, The log has been cleared.
2020/10/07-18:28:33, [SULB-1044], 3, SLOT 5 |CHASSIS, INFO, switch, Firmwaredownload to secondary partition
has completed successfully.
2020/10/07-18:28:36, [FSSM-1002], 4, SLOT 5 |CHASSIS, INFO, switch, HA State is in sync.
2020/10/07-18:28:39, [RAS-1007], 6, SLOT 5 |CHASSIS, INFO, switch, System is about to reload.
```

Displaying RASLog Messages by Message ID

To display RASLog messages based on message ID, perform the following steps:

1. Log in to the switch as admin.
2. Use the `errdump --message message_ID` command. The following example displays all instances of the messageHAM- 1004.

```
switch:admin> errdump --message HAM-1004
Fabric OS: 9.0.0
2020/10/07-18:29:59, [HAM-1004], 7, CHASSIS, INFO, switch, Processor rebooted - FirmwareDownload.
2018/02/09-12:37:38, [HAM-1004], 58, CHASSIS, INFO, switch, Processor rebooted - FirmwareDownload.
2020/10/14-11:38:35, [HAM-1004], 167, CHASSIS, INFO, Switch, Processor rebooted - FirmwareDownload. [...]
```

Displaying Messages on a Slot

To display the saved messages for a specific slot, perform the following steps:

1. Log in to the switch as admin.
2. Use the `errdump --slot slot_num` command.

```
switch:admin> errdump --slot 2
Fabric OS: 9.0.0a
2020/10/14-15:42:27, [HAM-1004], 85, SLOT 2 | CHASSIS, INFO, switch, Processor rebooted - HaFailover.
2020/10/14-15:42:27, [IPAD-1000], 86, SLOT 2 | CHASSIS, INFO, switch, SW/0 Ether/0 IPv6 manual
2620:100:0:f804:227:f8ff:fe2:c2a8/64 DHCP Off.
2020/10/14-15:42:27, [IPAD-1001], 88, SLOT 2 | CHASSIS, INFO, switch, CP/0 IPv6 manual
fe80::21b:edff:fe0f:b600 DHCP Off.
2020/10/14-15:42:27, [IPAD-1001], 89, SLOT 2 | CHASSIS, INFO, switch, CP/0 IPv6 manual
```

```
fe80::21b:edff:fe0c:bc00 DHCP Off. [...]
```

NOTE

The slot option is not supported on non-bladed systems.

Viewing RASLog Messages from Web Tools

To view the system message log for a switch from Web Tools, perform the following steps:

1. Launch Web Tools.
2. Select the desired switch from the Fabric Tree. The Switch View displays.
3. Click the Switch Events tab. You can view the switch events and messages in the Switch Events Report displayed.

In dual-domain switches, an Event button exists for each logical switch. Only messages relating to that switch (and chassis) is displayed.

Clearing System Message Logs

This section provides information on clearing system message logs. These procedures are valid for all supported platforms.

Clearing the System Message Log

To clear the system message log for a particular switch instance, perform the following steps:

1. Log in to the switch as admin.
2. Enter the `errClear` command to clear all messages from memory.

NOTE

For products that have a single processor, all error log messages are cleared. For products that have multiple processors, this command clears the error logs of only the processor from which it is issued.

Clearing the Audit Message Log

To clear the audit message log for a particular switch instance, perform the following steps:

1. Log in to the switch as admin.
2. Enter the `auditDump -c` command to clear all audit messages from memory.

Reading System Messages

This section provides information about reading the RASLog and audit messages.

Reading a RAS System Message

This section provides information about reading RAS system messages. The following example shows the format of a RAS system error message.

```
<timestamp>, [<Event ID>], <Sequence Number>, <Slot Number>, <Flags>, <Severity>, <Switch name>,
<Event-specific information>
```

The following example shows a sample message from the error log.

```
2018/02/27-15:36:22, [SS-1000], 629, SLOT 6 | CHASSIS, INFO, switch, supportSave has uploaded support
information to the remote host.
```

2018/02/27-17:00:02, [SS-1001], 631, SLOT 6 | CHASSIS, WARNING, switch, supportSave's upload operation to remote host has been aborted.

The fields in the error message are described in the below table:

Table 5: System Message Field Description

Variable Name	Description
Timestamp	The system time (UTC) when the message was generated on the switch. The RASLog subsystem supports an international timestamp format based on the "LOCAL" setting.
Event ID	The message module and number. These values uniquely identify each message in the Fabric OS and refer to the cause and recommended actions in this manual. Note that not all message numbers are used; there can be gaps in the numeric message sequence.
Sequence Number	The error message position in the log. When a new message is added to the log, this number is incremented by 1. The message sequence number starts at 1 after a firmwareDownload and will increase up to a value of 2,147,483,647 (0x7fffffff). The sequence number continues to increase after the message log wraps around; that is, the oldest message in the log is deleted when a new message is added. The sequence number can be reset to 1 using the errClear command. The sequence number persists across power cycles and switch reboots.
Slot Number	The slot/port number. On the fixed-port switches, ports are shown in port index format; on the chassis-based platforms, ports are shown in slot/port format.
Flags	For most messages, this field contains a space character (null value) indicating that the message is neither an AUDIT message nor an FFDC message. Messages may contain the following values: - FFDC—Indicates that additional First Failure Data Capture information has also been generated for this event. - FID—The fabric ID, which can range from 0 to 128. FID 128 means that the message was generated by the default switch instance. - CHASSIS—The message that was generated by the chassis instance. - PORT number—Indicates that the message was associated with the specific port identification number. - SLOT number—Indicates that the message was generated from the slot # blade main CPU. SLOT #/1—Indicates that the message was generated from the slot # blade Co-CPU.
Severity	The severity of the error, which can be one of the following: 1 – CRITICAL 2 – ERROR 3 – WARNING 4 – INFO
Switch name	The defined switch name or the chassis name of the switch depending on the action; for example, high availability (HA) messages typically show the chassis name, and login failures show the logical switch name. This variable takes only the first 16 characters and truncates the rest if it exceeds 16 characters in length. Run either the chassisName command to name the chassis or the switchName command to rename the logical switch.

Variable Name	Description
Event-specific information	A text string that explains the error encountered and provides parameters supplied by the software at runtime.

Reading an Audit Message

Compared to RASLog error messages, messages flagged as AUDIT provide additional user and system-related information of interest for post-event auditing and troubleshooting.

The following example shows the format of an audit event message.

```
<Sequence Number> AUDIT, <timestamp>, [<Event ID>], <Severity>, <Event Class>, <User ID>/<Role>/
<IP address>/<Interface>/<Application Name>, <Admin Domain>/<Switch name>, <Reserved field for
future expansion>, <Event-specific information>
```

For syslog audit messages, the Fabric OS version and six reserved fields are displayed in the message. The following is a sample audit event message.

```
0 AUDIT, 2005/12/10-09:54:03, [SEC-1000], WARNING, SECURITY, JohnSmith/admin/192.0.2.2/Telnet/CLI,
Domain A/JohnsSwitch, Incorrect password during login attempt.
```

The fields in the error message are described in the below table:

Table 6: Audit Message Field Description

Variable Name	Description
Sequence Number	The error message position in the log.
Audit flag	Identifies the message as an audit message.
Timestamp	The system time (UTC) when the message was generated on the switch. The RASLog subsystem supports an international timestamp format based on the "LOCAL" setting.
Event ID	The message module and number. These values uniquely identify each message in the Fabric OS and refer to the cause and recommended actions in this manual. Note that not all message numbers are used; there can be gaps in the numeric message sequence.
Severity	The severity of the error, which can be one of the following: • 1 – CRITICAL • 2 – ERROR • 3 – WARNING • 4 – INFO
Event Class	The event class, which can be one of the following: • CFG • CLI • FABRIC • FIRMWARE • LS • MAPS • RAS • SECURITY • ZONE

Variable Name	Description
User ID	The user ID.
Role	The role of the user.
IP address	The IP address.
Interface	The interface being used.
Application Name	The application name being used on the interface.
Admin Domain	The admin Domain, if there is one. From Fabric OS 9.1.0, support is provided to display the SANnav user name in the Audit Event Message format.
Switch name	The defined switch name or the chassis name of the switch depending on the action; for example, HA messages typically show the chassis name, and login failures show the logical switch name. This variable takes only the first 16 characters and truncates the rest if it exceeds 16 characters in length. Use the <code>chassisName</code> command to name the chassis or the <code>switchName</code> command to rename the logical switch.
Reserved field for future expansion	This field is reserved for future use and contains a space character (null value).
Event-specific information	A text string that explains the error encountered and provides parameters supplied by the software at runtime.

Responding to System Messages

This section provides procedures on gathering information about system messages.

Looking Up a System Message

Messages documented in this manual are arranged alphabetically by module ID and then numerically within a given module. To look up a message, copy down the module (refer to the [System Module Descriptions table](#)) and the error code and compare this information with the table of contents or lookup lists to determine the location of the information for that message.

The following information is provided for each message:

- Module and code name for the error
- Message text
- Message type
- Class (for audit messages only)
- Message severity
- Probable cause
- Recommended action

Gathering Information about the Problem

Ask yourself the following questions when troubleshooting a system message:

- What is the current Fabric OS level?
- What is the switch hardware version?
- Is the switch operational?
- Assess the impact and urgency:

- Is the switch down?
 - Is it a standalone switch?
 - Does the switch have logical switches defined?
 - How large is the fabric?
 - Is the fabric redundant?
 - Document the sequence of events:
 - What happened just prior to the problem?
 - Is the problem repeatable?
 - If so, what are the steps to reproduce the problem?
 - What configuration was in place when the problem occurred?
 - Did a failover occur?
 - Was security enabled?
 - Was POST enabled?
 - Are serial port (console) logs available?
 - Which CP was the master?
 - What and when were the last actions or changes made to the system?
- Common steps to follow when troubleshooting a system message:
- Use the `errDump` command on each logical switch.
 - Use the `supportFtp` command (as needed) to set up automatic FTP transfers, and then run the `supportSave` command.

Troubleshooting Files for Support Personnel

Fabric OS creates a number of files that can help support personnel troubleshoot and diagnose a problem. This section describes those files and how to access or save the information for support personnel.

Panic Dump and Core Dump Files

Fabric OS creates panic dump files and core dump files when there are problems in the Fabric OS kernel. You can view panic dump files using the `pdShow` command. These files can build up in the kernel partition (typically because of failovers) and might need to be periodically deleted or downloaded using the `supportSave` command.

The software watchdog process (SWD) is responsible for monitoring daemons that are critical to the function of a healthy switch. The SWD holds a list of critical daemons that ping the SWD periodically at a predetermined interval defined for each daemon. The ping interval is set at 133 seconds, with the exception of the Fabric Watch daemon and the IP Storage daemon, which ping the SWD every 333 seconds. (For a complete list of daemons, see KSWD entry in [System Module Descriptions table](#).)

If a daemon fails to ping the SWD within the defined interval or if the daemon terminates unexpectedly, the SWD dumps information to the panic dump files, which help to diagnose the fundamental cause of the unexpected failure.

Enter the `pdShow` command to view these files or the `supportSave` command to send them to a host workstation using FTP. The panic dump files and core dump files are intended for support personnel use only.

Trace Dumps

Fabric OS produces trace dumps when problems are encountered within Fabric OS modules. These files are intended for support personnel use only. You can use the `supportSave` or `supportFTP` commands to collect and send trace dump files to a specified remote location to provide to support when requested. Trace dumps must be enabled and set up on the switch to detect the first event. Note that there is only one trace buffer on a switch.

supportSave Command

The `supportSave` command can be used to send the output of the system messages (RASLog), the trace files, and the `supportShow` command to an off-switch storage location through FTP. Before running the `supportSave` command, you should set up the FTP parameters using the `supportFtp` command. The `supportShow` command runs a large number of dump and show commands to provide global output of the status of the switch. After the `supportSave` operation is completed, you must enter the `supportSave -R` command to remove all unwanted files. Refer to the *Brocade® Fabric OS® Command Reference Manual* for more information on these commands.

Troubleshooting FFDC

Each FFDC event will cause a file creation with file name of `RASLOG MessageID-YY-MMDDHHMMSS.ffdc` under `/core_files/ffdc_data` directory. This file will contain the data of consolelog, errdumpall, and tracedump info plus the CLI info defined by NS-1001 message.

For example the FFDC file `NS-1001-05-0614002021.ffdc` will be created when NS-1001 was generated by Fabos Name Service.

The files are also automatically transferred to the customer's FTP site (if auto FTP is enabled) and stored along with panic dump, core dump files and trace dumps.

System Module Descriptions

The System Module Descriptions table provides a summary of the system modules for which messages are documented in this manual; the system modules are listed alphabetically by name. A module is a subsystem in the Fabric OS. Each module generates a set of numbered messages.

Table 7: System Module Descriptions

System Module	Description
AG	Access Gateway (AG) allows multiple hosts (or HBAs) to access the fabric using fewer physical ports. Access Gateway mode transforms Brocade switches and embedded switches into a device management tool that is compatible with different types of fabrics, including Brocade-, Cisco-, and McDATA-based fabrics.
AN	Error or warning messages from the Bottleneck Detection module, including notification of detected bottlenecks.
ASVR	The ASVR module messages indicate any problems associated with the application server, including issues with registration of virtual machines and/or containers within the fabric.
AUTH	Authentication error messages indicate problems with the authentication module of the Fabric OS.
BCM	The BCM kernel module is a Linux driver that manages and indicates any problems associated with the Broadcom Ethernet switch for 10G/40G ports.
BL	BL error messages are a result of faulty hardware, transient out-of-memory conditions, ASIC errors, or inconsistencies in the software state between a blade and the environment monitor (EM) module.
BLS	Fibre Channel over IP port configuration messages over the Brocade 7800 and FX8-24 blade.
BLZ	BLZ module messages indicate any problems associated with Fibre Channel over IP (FCIP) datapath processing and configurations.
BM	Blade management error messages are a result of autoleveling firmware upgrades performed by the control processor (CP).

System Module	Description
C4	C4 error messages indicate problems with the 32Gb/s-capable FC module of the Fabric OS.
C5	C5 error messages indicate problems with the 64Gb/s-capable FC module of the Fabric OS.
CAL	Common Access Layer (CAL) provides an XML interface for configuring switch parameters in an object model.
CDR	Driver error messages.
CFS	Congestion Free SAN is used by the Traffic Optimizer feature to optimize SAN traffic by isolating traffic into different performance groups. Performance groups are automatically determined based on predefined attributes such as destination speed and priority, and they use a dedicated resource path within the fabric.
CH	Command history messages indicate when the clihistory command changes the behavior of recording the command line interface (CLI) session.
CHS	Error messages reporting the problems in the management of blades in different slots of the chassis.
CNM	Cluster Node Manager (CNM) is a software daemon module of Fabric OS. The messages from CNM indicate problems encountered by CNM, warnings, or information to the user of events.
CNMC	Controller Area Network Management Interface Controller (CANMIC) module is a software daemon module of Fabric OS. This module interacts with the Enclosure Manager through the CANMIC and reports information and error messages to the user.
CONF	Status messages for configUpload and configDownload operations.
CTAP	A user-space daemon that forwards non-performance-critical messages from the TAPE driver to the Crypto Virtual LUN Controller (CVLC) and Security Processor (SP), and vice versa. This module also maintains a cache of recently acquired keys, reducing requests to the key vault itself.
CVLM	Crypto Virtual LUN Manager (CVLM) is a software module of Fabric OS. CVLM messages indicate problems encountered by CVLM, warnings to alert the user, or information to the user.
ECC	Error Checking and Correction (ECC) error messages indicate single-bit and multiple-bit errors in dynamic random access memory (DRAM) devices. ECC is a technology that helps to correct memory errors.
EM	The Environmental Monitor (EM) manages and monitors the various field-replaceable units (FRUs), including the port cards, control processor (CP) blades, blower assemblies, power supplies, and World Wide Name (WWN) cards. The EM controls the state of the FRUs during system startup, hot-plug sequences, and fault recovery. The EM provides access to and monitors the sensor and status data from the FRUs and maintains the integrity of the system using the environmental and power policies. The EM reflects system status by CLI commands, system light-emitting diodes (LEDs), and status and alarm messages. The EM also manages some component-related data.
ERCP	Error Reporting Control Process (ERCP) messages capture the corenet and memory subsystem errors.
ESM	The Extension Services Module (ESM) provides management control and reporting for extension features such as FCIP and IPEX as well as their associated configurations.
ESS	Exchange Switch Support (ESS) error messages indicate problems with the ESS module of Fabric OS. ESS is an SW_ILS mechanism used by switches to exchange vendor and support information.
ESW	ESW error messages indicate problems with the Ethernet switch module of Fabric OS.
EVMD	EVMD is the event management module.
EXDP	Extension Data Path Processor feature provides the support for the extension platform where DP can have support for Warm memory.

System Module	Description
FABR	FABRIC refers to a network of Fibre Channel switches. The FABR error messages come from the fabric daemon. The fabric daemon follows the FC-SW-3 standard for the fabric initialization process, such as determining the E_Ports, assigning unique domain IDs to switches, creating a spanning tree, throttling the trunking process, and distributing the domain and alias lists to all switches in the fabric.
FABS	Fabric OS system driver module.
FBC	Firmware blade compatibility errors with the control processor (CP).
FCLG	The Fibre Channel Link Aggregation (FC-LAG) feature is introduced to provide the FC-LAG capability between the BSN switches and third-party devices that are configured in end-host mode. It provides the advantage of using all the physical links that are connected to the same switch and FI.
FCMC	Fibre Channel miscellaneous messages relate to problems with the physical layer used to send Fibre Channel traffic to and from the switch.
FCPD	The Fibre Channel Protocol daemon is responsible for probing the devices attached to the loop port. Probing is a process that the switch uses to find the devices attached to the loop ports and to update the Name Server with the information.
FCPH	The Fibre Channel Physical Layer module is used to send Fibre Channel traffic to and from the switch.
FCR	Fibre Channel router-related traffic and activity on the fabric or back-end fabric.
FICN	The FICN messages are generated during FICON emulation processing on an FCIP tunnel.
FICU	The FICON-CUP daemon handles communication with fibre connectivity (FICON) on IBM FICON storage devices. Errors to this module are usually initiation errors or indications that FICON-CUP prerequisites have not been met, such as a license key, core process ID (PID), and secure mode on the fabric.
FKLB	Fabric OS I/O kernel library module.
FLOD	FLOD is a part of the Fabric Shortest Path First (FSPF) protocol that handles synchronization of the link state database (LSDB) and propagation of the link state records (LSRs).
FSPF	Fabric Shortest Path First (FSPF) is a link state routing protocol that is used to determine how frames should be routed. These messages are about protocol errors.
FSS	The Fabric OS state synchronization framework provides facilities by which the active control processor (CP) can synchronize with the standby CP, enabling the standby CP to take control of the switch nondisruptively during failures and software upgrades. These facilities include version negotiation, state information transfer, and internal synchronization functions, enabling the transition from standby to active operation. FSS is defined both as a component and a service. A <i>component</i> is a module in the Fabric OS that implements a related set of functionality. A <i>service</i> is a collection of components grouped together to achieve a modular software architecture.
FSSM	The Fabric OS State Synchronization Management module is defined both as a component and a service. A <i>component</i> is a module in Fabric OS, that implements a related set of functionality. A <i>service</i> is a collection of components grouped together to achieve a modular software architecture.
FTC	Fabric Traffic Controller is the module responsible for traffic feedback to and from the fabric and connected devices. It handles the registration and delivery of Fabric Performance Impact Notifications (FPINs) and hardware congestion signals.
FV	Flow Vision provides end-to-end visibility into fabric performance. SAN administrators can monitor, troubleshoot, and identify problems in the traffic without disrupting the data path.
HAM	HAM is a user-space daemon responsible for high availability management.
HAMK	This is the kernel module for the High Availability Management (HAM) daemon.

System Module	Description
HIL	Hardware independent layer.
HLO	HLO is a part of the Fabric Shortest Path First (FSPF) protocol that handles the HELLO protocol between adjacent switches. The HELLO protocol is used to establish connectivity with a neighbor switch, to establish the identity of the neighbor switch, and to exchange FSPF parameters and capabilities.
HMON	Health monitor.
HTTP	HTTP error messages.
IPAD	System messages generated by the IP admin demon.
IPS	Fibre Channel over IP license, tunneling, and port-related messages.
ISNS	ISNS server and client status messages.
KAC	KAC error messages indicate problems associated with Fabric OS and external key vaults.

System Module	Description
KSWD	The kernel software watchdog (KSWD) watches daemons for unexpected terminations and “hang” conditions and informs the HAM module to take corrective actions such as failover or reboot. The following daemons are monitored by KSWD: • Access Gateway daemon (agd) • Alias Server daemon (asd) • ARR daemon (arrd) • Authentication daemon (authd) • Blade Manager daemon (bmd) • Cluster Node Manager daemon (cnmd) • Common Access Layer daemon (cald) • Diagnostics daemon (diagd) • Environment Monitor daemon (emd) • Event Manager daemon (evmd) • Exchange Switch Support daemon (essd) • FA-API rpc daemon (rpcd) • Fabric daemon (fabricd) • Fabric Device Management Interface daemon (fdmid) • Fibre Channel Protocol daemon (fcpd) • FICON CUP daemon (ficud) • FSPF daemon (fspfd) • IGMP daemon (igmpd) • Inter-fabric Routing daemon (iswitchd) • IP Storage daemon (ipsd) • ISNS Client daemon on CP (isnscd) • KAC daemon (kacd) • LFM daemon (lfmd) • Link Aggregation Group daemon (lagd) • Management Server daemon (msd) • MM daemon (mmd) • Name Server daemon (nsd) • Link Level Discovery Protocol daemon (lldpd) • Parity Data Manager daemon (pdmd) • Proxy daemon (proxyd) • PS daemon (psd) • RASLOG daemon (raslogd) • RCS daemon (rcsd) • RM daemon (rmd) • Security daemon (secd) • Sigma daemon (sigmad) • SNMP daemon (snmpd)
KSWD	SP Management daemon (spmd) SVP daemon (svpd) System Services Module daemon (ssmd) Time Service daemon (tsd) TRACE daemon (traced) Traffic daemon (trafd) UFCS daemon (ufcsd) VS daemon (vsd) Web Linker daemon (weblinkerd) Web Tools daemon (webd) ZONE daemon (zoned)
KTRC	Kernel RAS trace module.
LACP	LACP error messages indicate problems with the Link Aggregation Control Protocol module of Fabric OS.

System Module	Description
LFM	LFM error messages indicate problems with the Logical Fabric Manager module, which is responsible for making a logical switch use XISLs. This involves creating and managing LISLs in a logical fabric.
LIC	The License module indicated the problem with license installation and removal operations
LOG	RASLog subsystem.
LSDB	The link state database is a part of the FSPF protocol that maintains records on the status of port links. This database is used to route frames.
MAPS	The MAPS module identifies and reports anomalies associated with the various error counters, thresholds, and resources monitored on the switch.
MFIC	MS-FICON messages relate to Fibre Connection (FICON) installations. Fibre Connection control unit port (FICON-CUP) messages are displayed under the FICU module.
MM	MM messages indicate problems with the management modules.
MPTH	Multicast path uses the shortest Path First (SPF) algorithm to dynamically compute a broadcast tree.
MQ	Message queues are used for interprocess communication. Message queues allow many messages, each of variable length, to be queued. Any process or interrupt service routine (ISR) can write messages to a message queue. Any process can read messages from a message queue.
MS	The Management Service (MS) enables the user to obtain information about the Fibre Channel fabric topology and attributes by providing a single management access point. MS provides for both monitoring and control of the following servers: Fabric Configuration Server: Provides for the configuration management of the fabric. Unzoned Name Server: Provides access to Name Server information that is not subject to zone constraints. Fabric Zone Server: Provides access to and control of zone information.
NBFS	NBFSM is a part of the Fabric Shortest Path First (FSPF) protocol that handles a neighboring or adjacent switch's finite state machine (FSM). Input to the FSM changes the local switch from one state to another, based on specific events. For example, when two switches are connected to each other using an inter-switch link (ISL) cable, they are in the Init state. After both switches receive HELLO messages, they move to the Database Exchange state, and so on. NBFSM states are Down (0), Init (1), Database Exchange (2), Database Acknowledge Wait (3), Database Wait (4), and Full (5).
NS	Indicates problems with the simple Name Server module.
LLDP	Link Layer Discovery Protocol (LLDP) error messages indicate problems with the operation and configuration of the link layer discovery protocol.
PDM	Parity Data Manager (PDM) is a user-space daemon responsible for the replication of persistent configuration files from the primary partition to the secondary partition and from the active CP blade to the standby CP blade.
PDTR	PDTR messages indicate that panic dump trace files have been created.
PLAT	PLAT messages indicate hardware problems.
PMGR	A group of messages that relate to logical switch creation, deletion, and configuration.
PORT	PORT error messages refer to the front-end user ports on the switch. Front-end user ports are directly accessible by users to connect end devices or connect to other switches.
PS	The Performance Server daemon measures the amount of traffic between endpoints or traffic with particular frame formats, such as SCSI frames, IP frames, and customer-defined frames.
PSWP	The portswap feature and associated commands generate these error messages.
QOSD	Quality of Service daemon (QOSD) maintains the CEE-map configuration and applies it to a port in the ASIC. QoS specifies a priority value between 0 and 7 (inclusive) that can be used to differentiate the traffic.

System Module	Description
RAS	Informational messages when First Failure Data Capture (FFDC) events are logged to the FFDC log or when there is a roll-over warning.
RCS	The Reliable Commit Service daemon generates log entries when it receives a request from the zoning, security, or management server for passing data messages to switches in the fabric. RCS then requests reliable transport write and read (RTWR) to deliver the message. RCS also acts as a gatekeeper, limiting the number of outstanding requests for the Zoning, Security, or Management Server modules.
RPCD	The Remote Procedure Call daemon (RPCD) is used by Fabric Access for API-related tasks.
RTE	RTE is responsible for determining the correct paths for each ingress frame and populating the routing tables in the ASICs with this information. The ASICs then use the information available in the routing tables to determine the path that a particular ingress frame needs to take before it exits the switch.
RTWR	The Reliable Transmit With Response service helps deliver data messages to specific switches in the fabric or to all switches in the fabric. For example, if some switches are not reachable or are off line, RTWR returns an “unreachable” message to the caller, allowing the caller to take the appropriate action. If a switch is not responding, RTWR retries 100 times.
SCN	The internal State Change Notification daemon is used for state change notifications from the kernel to the daemons within Fabric OS.
SEC	The Security daemon generates security errors, warnings, or information during security-related data management or fabric merge operations. Administrators should watch for these messages to distinguish between internal switch and fabric operation errors and external attacks.
SLNK	Brocade Support Link (BSL) automates many support and troubleshooting activities for customer environments and provides additional insight through reports and analysis. When enabled, a switch automatically gathers and sends the encrypted Brocade device configuration, event information, and health and performance metrics to the Brocade Support Link Server (SLS) on a regular basis.
SNMP	Simple Network Management Protocol (SNMP) is a universally supported low-level protocol that allows simple get, get next, and set requests to go to the switch (acting as an SNMP agent). It also allows the switch to send traps to the defined and configured management station. Brocade switches support six management entities that can be configured to receive these traps.
SPM	Error messages that indicate problems with key or SP management.
SS	The supportSave command generates these error messages if problems are encountered.
SSLP	The SSLP module messages indicate problems associated with the launch of open SLP processes in the switch.
SULB	The software upgrade library provides the <code>firmwareDownload</code> command capability, which enables firmware upgrades to both CP blades with a single command and nondisruptive code load to all Fabric OS switches. These messages might display if there are problems during the <code>firmwareDownload</code> procedure. Most messages are informational only and are generated even during successful firmware download. For additional information, refer to the <i>Brocade® Fabric OS® Administration Guide</i> .
SWCH	These messages are generated by the switch driver module that manages a Fibre Channel switch instance.
SYSC	System Controller is a daemon that starts up and shuts down all Fabric OS modules in the proper sequence.
SYSM	General system messages.
TRCE	RAS TRACE error messages.

System Module	Description
TS	Time Service provides fabric time synchronization by synchronizing all clocks in the fabric to the clock time on the principal switch.
UCID	The UCID (Unified Configuration Infrastructure Daemon) module manages all the configurations of FCoE and Layer 2 protocols.
UCST	UCST is a part of the Fabric Shortest Path First (FSPF) protocol that manages the unicast routing table.
UFCS	The UFCS (Universal Fabric Configuration Service) module manages the distribution and merging of data for its client.
UPATH	UPATH is a part of the FSPF protocol that uses the SPF algorithm to dynamically compute a unicast tree.
USL	USL module error message indicated the specific interface operational errors.
VS	The VS module messages indicate problems or information associated with the Dynamic Fabric Provisioning feature, including commands associated with the fapwwn command and configurations.
WEBD	WEBD module messages indicate problems with the Web Tools module.
XTUN	XTUN messages are generated by the FCIP tunnel implementation. These messages indicate the status of FCIP tunnels, FCIP emulation events for FCP traffic, or FCIP debug information (FTRACE buffer status changes).
ZONE	Zone module messages indicate problems associated with the zoning features, including commands associated with aliases, zones, and configurations.

Fabric OS System Messages

This section provides information on all the Fabric OS system messages that are categorized under Audit, Log, and FFDC. All the error, event, and RASLog messages are listed under their respective modules, which are arranged alphabetically.

AG Messages

Access Gateway (AG) module messages.

AG-1001

Message

N_Port ID virtualization (NPIV) is not supported by fabric port connected to port <port number>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the N_Port ID virtualization (NPIV) capability is not supported by the fabric port to which the Access Gateway is connected.

Recommended Action

- Execute the `portCfgNpivPort` command to enable NPIV capability on the port connected to the Access Gateway.
- Some blades and ports in a switch may not support NPIV. NPIV functionality cannot be enabled on such ports, and they will not respond to NPIV requests. Refer to the *Brocade Fabric OS Access Gateway Administration Guide* for specific AG-compatibility requirements.
- On non-Brocade switches, refer to the manufacturer's documentation to determine whether the switch supports NPIV and how to enable NPIV on these types of switches.

AG-1002

Message

Unable to find alternate N_Port during failover for N_Port <port number>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that no other N_Port is configured or that the fabric was unstable during failover.

Recommended Action

Check whether an alternate N_Port is configured using the `portCfgShow` command.

If the message persists, execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

AG-1003**Message**

Unable to failover N_Port <port number>. Failover across different fabric is not supported.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the failover does not get blocked between two fabrics, although it is not a supported configuration.

Recommended Action

Configure two or more N_Ports to connect to the same fabric; then execute the `ag --failoverenable` command to enable failover on these N_Ports.

AG-1004**Message**

Invalid response to fabric login (FLOGI) request from the fabric for N_Port <port number> wwn <port wwn>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the fabric sent an invalid response to the FLOGI Extended Link Service (ELS) for the specified N_Port.

Recommended Action

Check the configuration of the fabric switch.

If the message persists, execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

AG-1005

Message

FDISC response was dropped because F_Port <port number> is offline.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the F_Port connected to the host is offline, which caused the Fabric Discovery (FDISC) response to drop.

Recommended Action

Check the configuration of the host connected to the specified F_Port.

AG-1006

Message

Access Gateway mode has been <message>.

Message Type

AUDIT | LOG

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that Access Gateway mode has been enabled or disabled.

Recommended Action

Execute the `ag --modeshow` command to verify the current status of Access Gateway mode.

AG-1007

Message

FLOGI response not received for the N_Port <port number> connected to the fabric.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the N_Port connected to the fabric switch is not online. The specified N_Port has been disabled.

Recommended Action

Check the connectivity between the Access Gateway N_Port and the fabric switch port.

AG-1008

Message

Invalid Port Login (PLOGI) response from the fabric on the N_Port <port number>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the fabric switch management server did not accept the N_Port Login (PLOGI) request sent by the Access Gateway.

Recommended Action

Check the configuration of the fabric switch connected to the Access Gateway.

If the message persists, execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

AG-1009

Message

Sending FLOGI failed on N_Port <port number>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that there was a failure sending a Fabric Login (FLOGI) request from the Access Gateway to the fabric switch.

Recommended Action

Check the configuration of the fabric switch connected to the Access Gateway.

If the message persists, execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

AG-1010**Message**

Sending PLOGI failed on N_Port <port number>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that there was a failure sending an N_Port Login (PLOGI) request from the Access Gateway to the fabric switch.

Recommended Action

Check the configuration of the fabric switch connected to the Access Gateway.

If the message persists, execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

AG-1011**Message**

Sending FDISC failed on N_Port <port number>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that there was a failure sending a discover F_Port service parameter request from the Access Gateway to the fabric switch.

Recommended Action

Check the configuration of the fabric switch connected to the Access Gateway.

If the message persists, execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

AG-1012**Message**

Sending logout (LOGO) request failed on N_Port <port number>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that there was a failure sending an N_Port logout request from the Access Gateway to the fabric switch.

Recommended Action

Check the configuration of the fabric switch connected to the Access Gateway.

If the message persists, execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

AG-1013**Message**

F_Ports mapped to N_Port <port number> failed over to other N_Port(s).

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the specified N_Port is failing over to other N_Ports connected to the same fabric.

Recommended Action

Execute the `ag --mapshow` command to display the updated F_Port-to-N_Port mapping.

AG-1014**Message**

Failing back F_Ports mapped to N_Port <port number>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the specified N_Port is failing back F_Ports mapped to it.

Recommended Action

Execute the `ag --mapshow` command to display the updated F_Port-to-N_Port mapping.

AG-1015**Message**

Unable to find online N_Ports to connect to the fabric.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that no other N_Port is configured or that all N_Ports are currently offline.

Recommended Action

Check whether any other N_Port is configured using the `portCfgShow` command.

If the message persists, execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

AG-1016

Message

Failing over F_Ports mapped to N_Port <port number> to other N_Port(s).

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the specified N_Port has failed to come online. All F_Ports mapped to this N_Port are failing over to other active N_Ports.

Recommended Action

Execute the `ag --mapshow` command to display the updated F_Port-to-N_Port mapping.

AG-1017

Message

No N_Port(s) are currently Online.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that no N_Ports are currently configured in the system or that all configured N_Ports have failed to come online.

Recommended Action

Execute the `switchShow` command to display the status of all ports in the system. Execute the `portCfgShow` command to display the list of ports currently configured as N_Ports.

AG-1018

Message

Host port should not be connected to port <port number> which is configured as N_Port.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that an initiator or target port is erroneously connected to a port configured for N_Port operation.

Recommended Action

Execute the `switchShow` command to display the status of all ports in the system. Execute the `portCfgShow` command to display the list of ports currently configured as N_Ports. Make sure that the host is connected to an F_Port.

AG-1019**Message**

Unable to failover N_Port <port number>. No other N_Port in port group:<pgid> is online.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that failover across port groups is not supported.

Recommended Action

Check whether an alternate N_Port is configured in the specified port group using the `ag --pgshow` command.

AG-1020**Message**

F_Ports to N_Ports route/mapping has been changed.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the F_Port-to-N_Port mapping has been changed because the switch has come online or some new N_Ports or F_Ports have come online.

Recommended Action

Execute the `ag --mapshow` command to display the updated F_Port-to-N_Port mapping.

AG-1021**Message**

Unable to do Preferred-Failover of F_Port <port number>. Failover across different fabric is not supported.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that failover across N_Ports connected to different fabrics is not supported.

Recommended Action

Change the preferred N_Port settings of the specified F_Port using the `ag --prefset` command.

Choose the preferred N_Port so that it is in the same fabric as the primary N_Port of this F_Port. Execute the `ag --show` command to check the fabric connectivity of the N_Ports.

AG-1022**Message**

F_Port <f_port> is failed over to its preferred N_Port <n_port>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the specified F_Port is failing over to its preferred N_Port.

Recommended Action

Execute the `ag --mapshow` command to display the updated F_Port-to-N_Port mapping.

AG-1023

Message

F_Port <f_port> mapped to offline N_Port <n_port> is failed over to its preferred N_Port <preferred port>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the specified N_Port has failed to come online. The F_Port mapped to this N_Port had its preferred set and is online.

Recommended Action

Execute the `ag --mapshow` command to display the updated F_Port-to-N_Port mapping.

AG-1024

Message

F_Port <f_port> is failed back to its preferred N_Port <n_port>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the specified N_Port is failing back F_Ports, which are failed over to some other N_Port.

Recommended Action

Execute the `ag --mapshow` command to display the updated F_Port-to-N_Port mapping.

AG-1025

Message

Port group of Slave N_Port <port number> is different than its Master N_Port <n_port>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the port groups of the master and slave N_Ports are different, while the trunk area assigned to the attached F_Ports on the edge switch is the same.

Recommended Action

Execute the `porttrunkarea --show` command on the attached switch to verify that the trunk area is assigned to all ports in the system, and execute the `porttrunkarea --enable` command to reconfigure the trunk area.

AG-1026

Message

Unable to handle the login request on port <port number> due to insufficient resources.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that there are insufficient resources to accept the login request.

Recommended Action

Execute the `configure` command on the Access Gateway switch and increase the number of allowed logins on the specified port.

If the message persists, execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

AG-1027

Message

Unable to handle this login request on port <port number> because NPIV capability is not enabled on this port.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that N_Port ID virtualization (NPIV) is not enabled on the specified port.

Recommended Action

Execute the `portCfgNpivPort` command on the Access Gateway switch to enable the NPIV capability on the port.

AG-1028**Message**

Device with Port WWN <port_name> tried to perform fabric login through port <f_port>, without having access permission.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the device does not have login access for the specified port as per the Advanced Device Security (ADS) policy set by the user.

Recommended Action

Add the device to the ADS allow list for the specified port using the `ag --adsadd` command.

AG-1029**Message**

Port Group (ID: <pgid>) has ports going to different fabrics.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates a misconfiguration.

Recommended Action

Connect all ports in the port group to the same fabric.

AG-1030

Message

N_Port <port number> has been determined to be unreliable.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the port goes online and offline often, and therefore the port is marked as unreliable.

Recommended Action

No action is required. The port will automatically be marked as reliable after a certain interval of time if the port toggling remains within the threshold limit.

AG-1031

Message

Loop Detected for device with Port WWN <port_name> connected to port <port number>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that a routing loop is detected for the device connected to the specified port.

Recommended Action

Check the device configuration.

AG-1032

Message

N_Port <port number> has recovered from an unreliable state.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the port state has been stable for the last 5 minutes.

AG-1033**Message**

F_Port to N_Port mapping has been updated for N_Port (<n_port>).

Message Type

AUDIT | LOG

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the F_Ports mapped to an N_Port have changed and that the configuration file has been updated.

AG-1034**Message**

F_Port cannot accept any more logins (<f_port>).

Message Type

AUDIT | LOG

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the F_Port has already logged in the maximum number of devices.

AG-1035

Message

Device (<wwn>) connected to F-port (<f_port>) cannot login as ALPA value is not available (<alpa>).

Message Type

AUDIT | LOG

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that a device has already used the specified arbitrated loop physical address (ALPA) value.

AG-1036

Message

Port <port number> is connected to a non-Brocade fabric with Persistent ALPA enabled. Check the admin guide for supported configuration.

Message Type

AUDIT | LOG

Message Class

CFG

Message Severity

WARNING

Probable Cause

Indicates that one of the ports is connected to a non-Brocade fabric.

Recommended Action

Refer to the *Brocade Fabric OS Access Gateway Administration Guide* for the supported configuration.

AG-1037

Message

Trunked N_Port (<n_port>) going offline. If switchshow CLI for the connected fabric switch port displays Persistently disabled: Area has been acquired, then check cabling: all trunked ports should be in same ASIC Port Group.

Message Type

AUDIT | LOG

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates incorrect cabling.

Recommended Action

If the `switchShow` command on the connected fabric switch port displays **Persistently disabled: Area has been acquired**, then check cabling on the Access Gateway. All trunked ports in a single trunk must belong to the same application-specific integrated circuit (ASIC) port group.

AG-1038

Message

Brocade 8000 ports are going to different fabrics, check N_Port (<n_port>).

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates a misconfiguration.

Recommended Action

Connect all ports in the port group to the same fabric.

AG-1039

Message

F_Port <Port that was reset> was reset because a WWN mapped device using it, through N_Port <Port who's state change caused the reset>, went offline.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the specified F_Port was reset because an N_Port went offline and the changes need to be propagated to all involved devices.

Recommended Action

No action is required. This port reset was not an error.

AG-1040

Message

PID of the devices connected to Port <port number> may have changed, as the port was toggled. Check EE monitor <Truncated message>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that N_Port ID virtualization (NPIV) assigns a new port ID (PID) each time the same port is disabled and then re-enabled. As the PID has changed, the end-to-end (EE) monitors installed with the previous PID stop functioning.

Recommended Action

Install new EE monitors with the new PID of the port to be monitored by using the `perfAddEEMonitor` command.

AG-1041

Message

Static F_Ports mapped to N_Port <port number> are disabled as Trunking is enabled on the N_Port.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that a trunk is enabled on the specified N_Port, and therefore the F_Port static mapping is disabled.

Recommended Action

Delete the static mapping on the Access Gateway using the `ag --staticdel` command or disable the trunk on the N_Port using the `switchCfgTrunkPort` command.

AG-1042**Message**

Sending ELS_PORT_OPEN failed on N_Port <port number>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that there was a failure sending an ELS_PORT_OPEN request from the Access Gateway to the fabric switch.

Recommended Action

Check the configuration of the fabric switch connected to the Access Gateway.

If the message persists, execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

AG-1043**Message**

Authentication cannot be negotiated with the connected switch/HBA and therefore disabling the Port <port number>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that authentication has failed on the specified port. A possible reason could be that the edge switch connected to Access Gateway is using firmware earlier than Fabric OS 7.1.0.

Recommended Action

Check the authentication configuration of the edge switch using the `authutil --show` command.

AG-1044**Message**

Port <Port Number> has been disabled because switch requires authentication when device authentication policy is set to ON.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that a device that does not support authentication has tried to log in to the switch when the device authentication policy is in the ON state on the switch.

Recommended Action

Enable authentication on the device or set the device authentication state to PASSIVE/OFF on the switch if it is not mandatory. Use the `authUtil` command to change the device authentication policy.

AG-1045**Message**

New port <nport> has same Port WWN as old port <fport> as part of duplicate Port WWN detection policy.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the specified new port has the same Port World Wide Name (PWWN) as the old port.

AG-1046

Message

D_Port test will not start due to error in removing mapping for the F_Port <port>. Retry after sometime.

Message Type

AUDIT | LOG

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that there is an error in removing the mapping for the specified port and that consequently there was a failure in starting the D_Port test.

Recommended Action

Retry the D_Port test after some time.

AG-1047

Message

Error in restoring one or all the mappings for the F_Port <port>. Add the mappings manually. Configured <Configured N-port>, Static <Static N-port> and Preferred <Preferred N-port>.

Message Type

AUDIT | LOG

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that there is an error in restoring the mapping for the specified port.

Recommended Action

Add the mappings to the port manually.

AG-1048

Message

Invalid N_Port online SCN on port <port>. Port state is already active.

Message Type

AUDIT | LOG

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the N_port online state change notification (SCN) has been received on the port, which has already logged in.

Recommended Action

If the message persists, execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

AG-1049

Message

Name of the port group <pgid> has been changed to <pgname> from <old_pgname>.

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the name of the Port Group has been changed.

AG-1050

Message

N-Ports <nports> are added to the Port Group <pgid>.

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the N_Port(s) have been added to the port group.

AG-1051

Message

N-Ports <nports> are deleted from the Port Group <pgid>.

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the N_Port(s) have been deleted from the port group.

AG-1052

Message

User defined Port Group <pgid> has been created with name <pgname> and <mode> mode.

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that a user-defined port group has been created.

AG-1053

Message

User defined Port Group <pgid> has been deleted.

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that a user-defined port group has been deleted.

AG-1054

Message

Operational mode <mode> has been enabled for Port Group <pgid>.

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the operational mode has been enabled for the port group.

AG-1055

Message

Operational mode <mode> has been disabled for Port Group <pgid>.

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the operational mode has been disabled for the port group.

AG-1056

Message

Device PWWN <wwn> has been cleared from the ALPA login table.

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the device Port World Wide Name (PWWN) entry has been cleared from the arbitrated loop physical address (ALPA) login table.

AG-1057

Message

Persistent ALPA has been enabled with <mode> mode.

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the persistent arbitrated loop physical address (ALPA) has been enabled with stringent/flexible mode.

AG-1058**Message**

Persistent ALPA has been disabled.

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the Persistent arbitrated loop physical address(ALPA) has been disabled.

AG-1059**Message**

Automap balance has been enabled for <port_type> in Port Group <pgid>.

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the automap balance has been enabled for N_Ports/F_Ports in the port group.

AG-1060

Message

Automap balance has been disabled for <port_type> in Port Group <pgid>.

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the automap balance has been disabled for N_Ports/F_Ports in the port group.

AG-1061

Message

Automap balance has been enabled for <port_type> in Auto Policy.

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the automap balance has been enabled for N_Ports/F_Ports in the Auto Policy.

AG-1062

Message

Automap balance has been disabled for <port_type> in Auto Policy.

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the automap balance has been disabled for N_Ports/F_Ports in the Auto Policy.

AG-1063**Message**

Failover has been enabled for N-Port <nport> in the Port Group <pgid>.

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that failover has been enabled for the N_Port in the switch.

AG-1064**Message**

Failover has been disabled for N-Port <nport> in the Port Group <pgid>.

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that failover has been disabled for the N_Port in the switch.

AG-1065

Message

Failback has been enabled for N-Port <nport> in the Port Group <pgid>.

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that failback has been enabled for the N_Port in the switch.

AG-1066

Message

Failback has been disabled for N-Port <nport> in the Port Group <pgid>.

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that failback has been disabled for the N_Port in the switch.

AG-1067

Message

N-Port <nport> has been set as Preferred N-Port for F-Port <fport>.

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the N_Port has been set as the preferred N_Port for the F_Port.

AG-1068**Message**

N-Port <nport> has been deleted as Preferred N-Port for F-Port <printf>.

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the N_Port has been deleted as the preferred N_Port for the F_Port.

AG-1069**Message**

Port <nport> has been configured as Primary N-Port (Device Mappings) for the device with WWN <wwn>.

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the port is configured as primary N_Port for the device.

AG-1070

Message

N-Port <nport> has been removed as Primary N-Port (Device Mappings) for the device with WWN <wwn>.

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the N_Port has been removed as primary N_Port for the device.

AG-1071

Message

Device with WWN <wwn> (Device Mappings) has been added to the Port Group <pgid>.

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the device has been added to the port group.

AG-1072

Message

Device with WWN <wwn> (Device Mappings) has been removed from the Port Group <pgid>.

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the device has been removed from the port group.

AG-1073**Message**

Static device mapping(s) are enabled for WWN <wwn>.

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the static device mappings are enabled for the given World Wide Name (WWN).

AG-1074**Message**

Static device mapping(s) are disabled for WWN <wwn>.

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the static device mappings are disabled for the given World Wide Name (WWN).

AG-1075

Message

Port <nport> has been configured as Failover N-Port (Device Mappings) for the device with WWN <wwn>.

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the port is configured as a failover N_Port for the device.

AG-1076

Message

N-Port <nport> has been removed as Failover N-Port (Device Mappings) for the device with WWN <wwn>.

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the N_Port has been removed as a failover N_Port for the device.

AG-1077

Message

Fabric Name Monitoring timeout value has been changed to (<seconds>) seconds.

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the Fabric Name Monitoring timeout value changed.

AG-1078**Message**

<wwn> devices are allowed on the Port <fport>.

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that all the devices or no devices are allowed on the port.

AG-1079**Message**

Device <wwn> is added to the allowed list on Port <fport>.

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the device has been added to the allowed list on the port.

AG-1080

Message

Device <wwn> is deleted from the allowed list on the Port <fport>.

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the device has been deleted from the allowed list on the port.

AG-1081

Message

The reliability counter value has been changed to <value>.

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the reliability counter value has been changed.

AG-1082

Message

The configured, static and preferred mappings for the N-Port <nport> have been saved.

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the configured, static, and preferred mappings for the N_Port have been saved.

AG-1083**Message**

The backed up mappings for the N-Port <nport> have been deleted.

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the backed-up mappings for the N_Port have been deleted.

AG-1084**Message**

<policy_name> policy is <policy_status>.

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

The user has changed the policy.

Recommended Action

Run `ag --policyshow` to display the current policy.

AG-1085**Message**

Message received on unexpected port -- `iu_sid=0x<source_id> iu_port=<port_in_frame> msg_port=<port_in_msg> l_fport=<fport_in_login_table> l_alpa=0x<alpa_in_login_table> l_nport=<nport_in_login_table>`.

Message Type

LOG

Message Severity

WARNING

Probable Cause

A frame was received on an unexpected port.

Recommended Action

Collect a supportsave as soon as possible and notify the device vendor.

AG-1086**Message**

Slow drain device `0x<PID of slow drain device>` connected to F-port (`<Fport>`) have been quarantined.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that all devices that are zoned with the slow-drain device have been quarantined.

Recommended Action

To check all affected devices zoned to the slow- drain device, use the `nszonemember` command in the edge fabric.

AG-1087**Message**

Slow drain device `0x<PID of slow drain device>` connected to F-port (`<Fport>`) have been unquarantined.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that all the devices that are zoned with the slow-drain device have been unquarantined.

Recommended Action

To check all affected devices zoned to the slow-drain device, use the nszonemember command in the edge fabric.

AG-1088**Message**

N_Port <port number> failed to login due to D_Port Configuration mismatch.

Message Type

LOG

Message Severity

ERROR

Probable Cause

N_Port fail to come up due to D_Port Configuration mismatch Between the Access Gateway and Fabric Switch.

Recommended Action

Please configure N_Port as static D_Port in Access Gateway or Clear the Static D_Port configuration from the Fabric Switch.

AG-1089**Message**

No N_Port(s) are currently Online in Port Group (<Port Group ID>).

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that no N_Ports are currently configured in the given Port Group or all configured N_Ports in given Port Group have failed to come online.

Recommended Action

Execute the `switchShow` command to display the status of all ports in the system. Execute the `portCfgShow` command to display the list of ports currently configured as N_Ports.

AG-1090**Message**

Use count of the IU that is received by AG port <port> is unexpected.

Message Type

LOG

Message Severity

ERROR

Probable Cause

To find the use count of the IU that is received by AG.

Recommended Action

Please execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

AG-1091**Message**

Invalid AC port SCN received on Port (<port>) which is not part of Trunk

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the AC Master port scn which is not in Trunk state.

Recommended Action

None.

AG-1092

Message

Applying N-Port configuration fails with reason code=<error> for Port=<port>

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates there is error in configuring port as N-port.

Recommended Action

Please execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

AG-1093

Message

N-Port <port> not permitted to come online as its connected to ICL port.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that N_ports were connected to the Core blades On Edge switch.

Recommended Action

Do not connect the N-Ports to the Core blades On Edge switch.

AG-1094

Message

ALPA Login table has been cleared for port <port>

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the device Port World Wide Name (PWWN) entries for a fport has been cleared from the arbitrated loop physical address (ALPA) login table.

AL Messages

Application Launcher error messages.

AL-1003

Message

Application <app name> is launched.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that an application is launched.

AL-1004

Message

Application <app name> is restarted.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that an application is restarted.

AL-1005

Message

Application <app name> is unexpected terminated.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that an application has been terminated unexpectedly.

AL-1006

Message

Application <app name> is stopped.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that an application has been stopped by the user.

AN Messages

Error or warning messages from the Bottleneck Detection module.

AN-1001

Message

Failed to allocate memory: (<function name>).

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the specified function has failed to allocate memory.

Recommended Action

Check memory usage on the switch using the `memShow` command. Restart or power-cycle the switch.

AN-1002**Message**

Failed to initialize; rc = <error>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the initialization of the "trafd" daemon has failed.

Recommended Action

Download a new firmware version using the `firmwareDownload` command.

AN-1010**Message**

Severe latency bottleneck detected at <Port Type> <slotport string>.

Message Type

LOG | AUDIT

Message Class

FABRIC

Message Severity

WARNING

Probable Cause

Indicates credit loss at the specified port, a downstream port, or a very high latency device at the edge of the fabric.

Recommended Action

Contact your switch service provider for assistance.

AN-1011

Message

Could not distinguish between primary and dependent severe latency bottleneck on port <slotport string> because port mirroring is enabled on this port.

Message Type

LOG | AUDIT

Message Class

FABRIC

Message Severity

WARNING

Probable Cause

Indicates that resources that are needed to determine whether there is complete credit loss on a virtual channel (VC) at the specified port are used by port mirroring.

Recommended Action

Contact your switch service provider for assistance.

AN-1012

Message

Credits did not return from other end. Complete loss of credits on a VC on port <slotport string>.

Message Type

LOG | AUDIT

Message Class

FABRIC

Message Severity

WARNING

Probable Cause

Indicates a credit loss.

Recommended Action

If this message is not followed by the AN-1013 message, contact your switch service provider for assistance.

AN-1013

Message

Performed link reset to recover the port credits on port <slotport string>.

Message Type

LOG | AUDIT

Message Class

FABRIC

Message Severity

INFO

Probable Cause

Indicates a credit loss.

Recommended Action

The port is recovered. No action is required.

AN-1014

Message

Frame <frametype> detected, tx port <tx slotport string> rx port <rx slotport string>, sid <sid>, did <did>, timestamp <timestamp>.

Message Type

LOG | AUDIT

Message Class

FABRIC

Message Severity

INFO

Probable Cause

Indicates a C3 discard frame.

Recommended Action

Check the *Brocade Fabric OS Troubleshooting and Diagnostics User Guide* for troubleshooting information or contact your switch service provider if the message persists.

ASVR Messages

Application Sever Virtual Registration error messages.

ASVR-1001

Message

Maximum VM registrations exceeded for PID 0x<pid>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the host adapter has attempted to register a greater number of virtual machines than is supported.

Recommended Action

Configure fewer virtual machines on the host at the specified port ID (PID).

AUTH Messages

Authentication error messages.

AUTH-1001

Message

<Operation type> has been successfully completed.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the secret database operation has been updated using the `secAuthSecret` command. The values for the operation type can be "set" or "remove".

AUTH-1002

Message

<Operation type> has failed.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the specified action has failed to update the secret database using the `secAuthSecret` command. The values for the operation type can be "set" or "remove".

Recommended Action

Execute the `secAuthSecret` command again.

If the message persists, execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

AUTH-1003**Message**

<data type> type has been successfully set to <setting value>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that an authentication configuration value was set to a specified value. The data type is authentication type, DH group type, hash type, or policy type.

AUTH-1004**Message**

Failed to set <data type> type to <setting value>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the `authUtil` command has failed to set the authentication configuration value. The data type can be authentication type, DH group type, hash type, or policy type.

Recommended Action

Execute the `authUtil` command again.

If the message persists, execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

AUTH-1005**Message**

Authentication file does not exist: <error code>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates an authentication file corruption.

Recommended Action

Execute the `firmwareDownload` command to reinstall the firmware.

If the message persists, execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

AUTH-1006**Message**

Failed to open authentication configuration file.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates an internal problem with the Secure Fabric OS.

Recommended Action

Reinitialize authentication using the `portDisable` and `portEnable` commands or the `switchDisable` and `switchEnable` commands.

If the message persists, execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

AUTH-1007**Message**

The proposed authentication protocol(s) are not supported: port <port number>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the proposed authentication protocol types are not supported by the specified local port.

Recommended Action

Execute the `authUtil` command to make sure that the local switch supports the Fibre Channel Authentication Protocol (FCAP) or Diffie-Hellman Challenge Handshake Protocol (DHCHAP) protocols.

AUTH-1008**Message**

No security license, operation failed.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the switch does not have a security license.

Recommended Action

Verify that the security license is installed using the `licenseShow` command. If necessary, reinstall the license using the `licenseAdd` command.

AUTH-1010

Message

Failed to initialize security policy: switch <switch number>, error <error code>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates an internal problem with the Secure Fabric OS.

Recommended Action

Reboot or power-cycle the switch.

If the message persists, execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

AUTH-1011

Message

Failed to register for failover operation: switch <switch number> error <error code>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates an internal problem with the Secure Fabric OS.

Recommended Action

Reinitialize authentication using the `portDisable` and `portEnable` commands or the `switchDisable` and `switchEnable` commands.

If the message persists, execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

AUTH-1012

Message

Authentication <code> is rejected: port <port number> explain <explain code> reason <reason code>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the specified authentication is rejected because the remote entity does not support authentication.

Recommended Action

Verify the hash type, protocol, group, and authentication policy using the `authutil --show` command.

AUTH-1013

Message

Cannot perform authentication request message: port <port number>, message code <message code>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the system is running low on resources when receiving an authentication request. Usually this problem is transient. The authentication may fail.

Recommended Action

Reinitialize authentication using the `portDisable` and `portEnable` commands or the `switchDisable` and `switchEnable` commands.

If the message persists, execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

AUTH-1014

Message

Invalid port value to <operation>: port <port number>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates an internal problem with the Secure Fabric OS.

Recommended Action

Reinitialize authentication using the `portDisable` and `portEnable` commands or the `switchDisable` and `switchEnable` commands.

If the message persists, execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

AUTH-1016

Message

Invalid value to start HBA authentication port: <port number>, pid <pid>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates an internal failure.

Recommended Action

Copy the message and collect the switch information using the `supportShow` command, and contact your switch service provider.

AUTH-1017

Message

Invalid value to start authentication request: port <port number>, operation code <operation code>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates an internal problem with the Secure Fabric OS.

Recommended Action

Reinitialize authentication using the `portDisable` and `portEnable` commands or the `switchDisable` and `switchEnable` commands.

If the message persists, execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

AUTH-1018

Message

Invalid value to check protocol type: port <port number>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates an internal problem with the Secure Fabric OS.

Recommended Action

Reinitialize authentication using the `portDisable` and `portEnable` commands or the `switchDisable` and `switchEnable` commands.

If the message persists, execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

AUTH-1020

Message

Failed to create timer for authentication: port <port number>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that an authentication message timer was not created. Usually this problem is transient. The authentication may fail.

Recommended Action

Reinitialize authentication using the `portDisable` and `portEnable` commands or the `switchDisable` and `switchEnable` commands.

If the message persists, execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

AUTH-1022**Message**

Failed to extract <data type> from <message> payload: port <port number>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the authentication process failed to extract a particular value from the receiving payload. Usually this problem is transient. The authentication may fail.

Recommended Action

Reinitialize authentication using the `portDisable` and `portEnable` commands or the `switchDisable` and `switchEnable` commands.

If the message persists, execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

AUTH-1023**Message**

Failed to <operation type> during <authentication phase>: port <port number>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that an authentication operation failed for a certain authentication phase. The operation type varies depending on authentication type:

- Some operations for Switch Link Authentication Protocol (SLAP): certificate retrieve, certificate verification, signature verification, or nonce signing.
- Some operations for Fibre Channel Authentication Protocol (FCAP): certificate retrieve, certificate verification, signature verification, or nonce signing.
- Some operations for Diffie-Hellman Challenge Handshake Authentication Protocol (DHCHAP): response calculation, challenge generation, or secret retrieve.

The authentication phase specifies which phase of a particular authentication protocol failed.

A nonce is a single-use, usually random value used in authentication protocols to prevent replay attacks.

Recommended Action

The error may indicate that an invalid entity tried to connect to the switch. Check the connection port for a possible unauthorized access attack.

It may indicate that the public key infrastructure (PKI) object for SLAP or FCAP or the secret value for DHCHAP on the local entity is not set up properly. Reinstall all PKI objects or reset the secret value for DHCHAP properly.

If the message persists, execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

AUTH-1025

Message

Failed to get <data type> during <authentication phase>: port <port number>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the authentication process failed to get expected information during the specified authentication phase. Usually this problem is transient. The authentication may fail.

Recommended Action

Reinitialize authentication using the `portDisable` and `portEnable` commands or the `switchDisable` and `switchEnable` commands.

If the message persists, execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

AUTH-1026

Message

Failed to <Device information> during negotiation phase: port <port number>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the authentication failed to get device or host bus adapter (HBA) information due to an internal failure. Usually this problem is transient. If the authentication failed, retry the login.

Recommended Action

Reinitialize authentication using the `portDisable` and `portEnable` commands or the `switchDisable` and `switchEnable` commands.

If the message persists, execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

AUTH-1027

Message

Failed to select <authentication value> during <authentication phase>: value <value> port <port number>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the authentication process failed to select an authentication value (DH group, hash value, or protocol type) from a receiving payload for a particular authentication phase. This indicates that the local switch does not support the specified authentication value.

Recommended Action

Check the authentication configuration and reset the supported value if needed using the `authUtil` command.

Reinitialize authentication using the `portDisable` and `portEnable` commands or the `switchDisable` and `switchEnable` commands.

If the message persists, execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

AUTH-1028

Message

Failed to allocate <data type> for <operation phase>: port <port number>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the authentication process failed because the system is low on memory. Usually this problem is transient. The authentication may fail.

The data type is the payload or structure that failed to get memory. The operation phase specifies which operation of a particular authentication phase failed.

Recommended Action

Reinitialize authentication using the `portDisable` and `portEnable` commands or the `switchDisable` and `switchEnable` commands.

If the message persists, execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

AUTH-1029

Message

Failed to get <data type> for <message phase> message: port <port number>, retval <error code>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the authentication process failed to get a particular authentication value at a certain phase. Usually this problem is transient. The authentication may fail.

The data type is the payload or structure that failed to get memory.

Recommended Action

Reinitialize authentication using the `portDisable` and `portEnable` commands or the `switchDisable` and `switchEnable` commands.

If the message persists, execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

AUTH-1030**Message**

Invalid message code for <message phase> message: port <port number>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the receiving payload does not have a valid message code for a particular authentication phase. Usually this problem is transient. The authentication may fail.

Recommended Action

Reinitialize authentication using the `portDisable` and `portEnable` commands or the `switchDisable` and `switchEnable` commands.

If the message persists, execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

AUTH-1031**Message**

Failed to retrieve secret value: port <port number>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the secret value was not set properly for the authenticated entity.

Recommended Action

Reset the secret value using the `secAuthSecret` command.

Reinitialize authentication using the `portDisable` and `portEnable` commands or the `switchDisable` and `switchEnable` commands.

If the message persists, execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

AUTH-1032**Message**

Failed to generate <data type> for <message payload> payload: length <data length>, error code <error code>, port <port number>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the authentication process failed to generate specific data (challenge, nonce, or response data) for an authentication payload. This usually relates to an internal failure.

A nonce is a single-use, usually random value used in authentication protocols to prevent replay attacks.

Usually this problem is transient. The authentication may fail.

Recommended Action

Reinitialize authentication using the `portDisable` and `portEnable` commands or the `switchDisable` and `switchEnable` commands.

If the message persists, execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

AUTH-1033**Message**

Disable port <port number> due to unauthorized switch <switch WWN value>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that an entity was not configured in the Switch Connection Control (SCC) policy and tried to connect to the port.

Recommended Action

Add the World Wide Name (WWN) of the entity to the SCC policy and reinitialize authentication by using the `portDisable` and `portEnable` commands or the `switchDisable` and `switchEnable` commands.

AUTH-1034**Message**

Failed to validate name <entity name> in <authentication message>: port <port number>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the specified entity name in the payload is not in the correct format.

Recommended Action

Reinitialize authentication using the `portDisable` and `portEnable` commands or the `switchDisable` and `switchEnable` commands.

If the message persists, execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

AUTH-1035**Message**

Invalid <data type> length in <message phase> message: length <data length>, port <port number>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that a particular data field in the authentication message has an invalid length field. This error usually relates to an internal failure. Usually this problem is transient. The authentication may fail.

Recommended Action

Reinitialize authentication using the `portDisable` and `portEnable` commands or the `switchDisable` and `switchEnable` commands.

If the message persists, execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

AUTH-1036**Message**

Invalid state <state value> for <authentication phase>: port <port number>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the switch received an unexpected authentication message. Usually this problem is transient. The authentication may fail.

Recommended Action

Reinitialize authentication using the `portDisable` and `portEnable` commands or the `switchDisable` and `switchEnable` commands.

If the message persists, execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

AUTH-1037**Message**

Failed to <operation type> response for <authentication message>: init_len <data length>, resp_len <data length>, port <port number>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that a Diffie Hellman - Challenge Handshake Authentication Protocol (DH-CHAP) authentication operation failed on the specified port due to mismatched response values between two entities or due to same secret in all the entities.

The error may indicate that an invalid entity tried to connect to the switch. Check the connection port for a possible security attack.

Recommended Action

Reinitialize authentication using the `portDisable` and `portEnable` commands or the `switchDisable` and `switchEnable` commands.

If the message persists, execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

AUTH-1038

Message

Failed to retrieve certificate during <authentication phase>: port <port number>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the public key infrastructure (PKI) certificate is not installed properly.

Recommended Action

Reinstall the PKI certificate using the `secCertMgmt` command.

Reinitialize authentication using the `portDisable` and `portEnable` commands or the `switchDisable` and `switchEnable` commands.

If the message persists, execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

AUTH-1039

Message

Neighboring switch has conflicting authentication policy: Port <Port Number> disabled.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the neighboring switch has a conflicting authentication policy enabled. The E_Port has been disabled because the neighboring switch has rejected the authentication negotiation, and the local switch has a strict switch authentication policy.

Recommended Action

Correct the switch policy configuration on either of the switches using the `authUtil` command, and then enable the port using the `portEnable` command.

AUTH-1040**Message**

Reject authentication on port <Port Number>, because switch authentication policy is set to OFF.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the local switch has rejected the authentication because the switch policy is turned off. If the neighboring switch has a strict (ON) switch policy, the port will be disabled due to conflicting configuration settings. Otherwise, the E_Port will form without authentication.

Recommended Action

If the port is disabled, correct the switch policy configuration on either of the switches using the `authUtil` command, and then enable the port on the neighboring switch using the `portEnable` command. If the E_Port has formed, no action is required.

AUTH-1041**Message**

Port <port number> has been disabled, because an authentication-reject was received with code '<Reason String>' and explanation '<Explanation String>'.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the specified port has been disabled because it received an authentication-reject response from the connected switch or device. The error may indicate that an invalid entity tried to connect to the switch.

Recommended Action

Check the connection port for a possible security attack.

Check the shared secrets using the `secAuthSecret` command, and reinitialize authentication using the `portDisable` and `portEnable` commands.

If the message persists, execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

AUTH-1042**Message**

Port <port number> has been disabled, because authentication failed with code '<Reason String>' and explanation '<Explanation String>'.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the specified port has been disabled because the connecting switch or device failed to authenticate. The error may indicate that an invalid entity attempted to connect to the switch.

Recommended Action

Check the connection port for a possible security attack.

Check the shared secrets using the `secAuthSecret` command, and reinitialize authentication using the `portDisable` and `portEnable` commands.

If the message persists, execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

AUTH-1043**Message**

Failed to enforce device authentication mode:<Device Auth Policy>(error: <Reason Code>).

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the Kernel mode setting for F_Port authentication failed. Device authentication will be defaulted to OFF, and the switch will not participate in Diffie-Hellman Challenge Handshake Authentication Protocol (DHCHAP) authentication with other devices.

Recommended Action

Set the device authentication policy manually using the `authUtil` command.

AUTH-1044**Message**

Authentication <Reason for disabling the port>. Disabling the port <port number>.

Message Type

LOG | FFDC

Message Severity

ERROR

Probable Cause

Indicates that authentication has timed out after multiple retries. The specified port has been disabled as a result. This problem may be transient due to the system CPU load. In addition, a defective small form-factor pluggable (SFP) transceiver or faulty cable may have caused the failure.

Recommended Action

Check the SFP transceiver and the cable; then enable the port using the `portEnable` command.

AUTH-1045**Message**

Certificate not present in this switch in <authentication phase> port <port number>.

Message Type

AUDIT | LOG

Message Class

SECURITY

Message Severity

WARNING

Probable Cause

Indicates that the public key infrastructure (PKI) certificate is not installed in this switch.

Recommended Action

If DHCHAP authentication is also configured and the port is authenticated, no action is needed. Otherwise, check the certificate availability using the `secCertMgmt show -cert fcap` command.

Install the certificate and reinitialize authentication using the `portDisable` and `portEnable` commands or the `switchDisable` and `switchEnable` commands.

If the message persists, execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

AUTH-1046

Message

<Operation type> has been successfully completed.

Message Type

AUDIT | LOG

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates that the certificate database operation has been updated using the `secAuthCertificate` command. The values for operation type can be "set" or "remove".

AUTH-1047

Message

<Operation type> has failed.

Message Type

AUDIT | LOG

Message Class

SECURITY

Message Severity

ERROR

Probable Cause

Indicates that the specified action has failed to update the certificate database using the `secAuthCertificate` command. The values for operation type can be "set" or "remove".

Recommended Action

Execute the `secAuthCertificate` command again.

If the message persists, execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

AUTH-1048**Message**

Stopping synchronization of the system due to <Operation type> incompatibility with standby CP.

Message Type

AUDIT | LOG

Message Class

SECURITY

Message Severity

ERROR

Probable Cause

Indicates that the software version on the standby control processor (CP) is incompatible with this software feature enabled in the Fabric OS firmware version because the in-flight encryption feature supports both DHCHAP and FCAP protocols.

Recommended Action

Upgrade the software on the standby CP or disable the software feature on this CP.

To allow standby synchronization, use the DHCHAP protocol only for in-flight encryption, and disable the FCAP protocol in `authutil`. Use the `authutil --set -a "protocol type"` command to configure the DHCHAP protocol.

AUTH-1049**Message**

Slave port <Slave port number> has been disabled, as Master port <Master port number> was disabled because of authentication failure/rejection.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the specified slave port has been disabled because it received an authentication-reject response from the connected switch or device. The error informs that the slave port is disabled due to a master port authentication failure or rejection.

Recommended Action

Check the connection port for a possible security attack.

Check the shared secrets using the `secAuthSecret` command, or check the certificates using the `secCertMgmt` command, and reinitialize authentication using the `authutil --authinit` command.

If the message persists, execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

AUTH-1050**Message**

Port <port number> has been reset, because authentication stage is conflicted with the peer.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the specified port has been reset because there is a conflicting authentication stage with the connected switch or device. The error may indicate that an invalid entity attempted to connect to the switch.

Recommended Action

Check the connection port for a possible security attack.

If the message persists, execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

AUTH-1051**Message**

Reject authentication on port <Port Number>, because device authentication policy is set to OFF.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the local switch has rejected the authentication because the device policy is turned off. Otherwise, the F_Port will form without authentication.

Recommended Action

If the port is disabled, correct the device policy configuration on the switch using the `authUtil` command. If the F_Port has formed, no action is required.

AUTH-3001**Message**

Event: <Event Name>, Status: success, Info: <Data type> type has been changed from [<Old value>] to [<New value>].

Message Type

AUDIT

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates that an authentication configuration value was set to a specified value. The data type can be authentication type, DH group type, hash type, or policy type.

AUTH-3002**Message**

Event: <Event Name>, Status: success, Info: <Event Related Info>.

Message Type

AUDIT

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates that the secret database operation has been updated using the `secAuthSecret` command.

AUTH-3003**Message**

Event: <Event Name>, Status: success, Info: <Operation type> the PKI objects.

Message Type

AUDIT

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates that the public key infrastructure (PKI) objects were created using the `secCertUtil` command or that the PKI objects were removed using the `secCertUtil delete -fcapall` command. The operation type can be either "Created" or "Removed".

AUTH-3004**Message**

Event: <Event Name>, Status: failed, Info: Neighboring switch has a conflicting authentication policy; Port <Port Number> disabled.

Message Type

AUDIT

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates that the specified E_Port was disabled because the neighboring switch rejected the authentication negotiation, and the local switch has a strict switch authentication policy.

Recommended Action

Correct the switch policy configuration on either of the switches using the `authUtil` command, and then enable the port using the `portEnable` command.

AUTH-3005**Message**

Event: <Event Name>, Status: failed, Info: Rejecting authentication request on port <Port Number> because switch policy is turned OFF.

Message Type

AUDIT

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates that the local switch has rejected the authentication request, because the switch policy is turned off. If the neighboring switch has a strict (ON) switch policy, the port will be disabled due to conflicting configuration settings. Otherwise, the E_Port will form without authentication.

Recommended Action

If the specified port is disabled, correct the switch policy configuration on either of the switches using the `authUtil` command, and then enable the port on the neighboring switch using the `portEnable` command. If the E_Port formed, no action is required.

AUTH-3006**Message**

Event: <Event Name>, Status: failed, Info: Authentication failed on port <port number> due to mismatch of DHCHAP shared secrets.

Message Type

AUDIT

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates that a Diffie-Hellman Challenge Handshake Authentication Protocol (DHCHAP) authentication operation failed on the specified port due to mismatched response values between two entities.

The error may indicate that an invalid entity tried to connect to the switch.

Recommended Action

Check the connection port for a possible security attack.

Check the shared secrets using the `secAuthSecret` command and reinitialize authentication using the `portDisable` and `portEnable` commands.

If the message persists, execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

AUTH-3007**Message**

Event: <Event Name>, Status: failed, Info: Port <port number> disabled due to receiving an authentication reject with code '<Reason String>' and Explanation '<Explanation String>'.

Message Type

AUDIT

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates that the specified port was disabled because it received an authentication-reject response from the connected switch or device.

The error may indicate that an invalid entity tried to connect to the switch.

Recommended Action

Check the connection port for a possible security attack.

Check the shared secrets using the `secAuthSecret` command and reinitialize authentication using the `portDisable` and `portEnable` commands.

If the message persists, execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

AUTH-3008

Message

Event: <Event Name>, Status: failed, Info: Port <port number> has been disabled due to authentication failure with code '<Reason String>' and explanation '<Explanation String>'.

Message Type

AUDIT

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates that the specified port has been disabled because the connecting switch or device failed to authenticate.

The error may indicate that an invalid entity tried to connect to the switch.

Recommended Action

Check the connection port for a possible security attack.

Check the shared secrets using the `secAuthSecret` command, and reinitialize authentication using the `portDisable` and `portEnable` commands.

If the message persists, execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

AUTH-3009

Message

Verification failed for certificate: <Certificate name>, error=<OpenSSL error string for verification error> at depth=<Depth of the error>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates an issue with the certificate.

Recommended Action

Check the time validity and correctness from the import time of the certificate using the `seccertmgmt` command.

If the issue persists, check with the certificate authority to examine the invalid certificate.

AUTH-3010**Message**

Certificate <Certificate name>, <OpenSSL error string for verification error with x509_strict option> at depth=<Depth of the error> (ignored).

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates benign issue with the certificate, warning to the user.

Recommended Action

Check the certificate well-formedness and compliance with RFC 5280.

If the issue persists, check with the certificate authority to examine the invalid certificate.

BCM Messages

BCM kernel module error messages.

BCM-1000**Message**

<command name> of GE <port number> failed. Please retry the command. Data: inst=<ASIC instance> st=<ASIC initializing state> rsn=<reason code> fn=<message function> oid=<ASIC ID>.

Message Type

LOG | FFDC

Message Severity

ERROR

Probable Cause

Indicates that the hardware is not responding to a command request, possibly because it is busy.

Recommended Action

Retry the command.

BCM-1001**Message**

FIPS <FIPS Test Name> failed; algo=<algorithm code> type=<algorithm type> slot=<Slot Number>.

Message Type

LOG | FFDC

Message Severity

CRITICAL

Probable Cause

Indicates that a Federal Information Protection Standard (FIPS) failure has occurred and requires faulting the blade or switch.

Recommended Action

Retry the command.

BCM-1002**Message**

An IPsec/IKE policy was added.

Message Type

AUDIT | LOG

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that an Internet Protocol Security (IPsec) or Internet Key Exchange (IKE) policy was added and the configuration file was updated.

BCM-1003

Message

An IPsec/IKE policy was deleted.

Message Type

AUDIT | LOG

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that an Internet Protocol Security (IPsec) or Internet Key Exchange (IKE) policy was deleted and the configuration file was updated.

BCM-1004

Message

Tape Read Pipelining is being disabled slot (<slot number>) port (<user port index>) tunnel (<The configured tunnel ID (0-7)>).

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the Fabric OS version on the remote end of the tunnel does not support Tape Read Pipelining.

BCM-1005

Message

S<slot number>,P<user port index>(<blade index>) [OID 0x<port OID>]: <string name of ge>: port faulted due to SFP validation failure. Please check if the SFP is valid for the configuration.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates a deteriorated small form-factor pluggable (SFP) transceiver, an incompatible SFP transceiver pair, or a faulty cable between the peer ports.

Recommended Action

Verify that compatible SFP transceivers are used on the peer ports (execute the `sfpShow` command on each side to verify a matched pair), that the SFP transceivers have not deteriorated, and that the Fibre Channel cable is not faulty. Replace the SFP transceivers or the cable if necessary.

BCM-1006**Message**

SLOT <slot number> UNIT <unit> [OID 0x<OID>]:<chip error string>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Possibly caused by uncontrolled CP failover.

Recommended Action

Please powercycle slot to recover blade.

BCMG Messages

BCMG module error messages.

BCMG-1000**Message**

<command name> of GE <port number> failed. Please retry the command. Data: inst=<ASIC instance> st=<ASIC initializing state> rsn=<reason code> fn=<message function> oid=<ASIC ID>.

Message Type

LOG | FFDC

Message Severity

ERROR

Probable Cause

Indicates that the hardware is not responding to a command request, possibly because it is busy.

Recommended Action

Retry the command.

BCMG-1001

Message

FIPS <FIPS Test Name> failed; algo=<algorithm code> type=<algorithm type> slot=<Slot Number>.

Message Type

LOG | FFDC

Message Severity

CRITICAL

Probable Cause

Indicates that a Federal Information Protection Standard (FIPS) failure has occurred and requires faulting the blade or switch.

Recommended Action

Retry the command.

BCMG-1002

Message

An IPsec/IKE policy was added.

Message Type

AUDIT | LOG

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that an Internet Protocol Security (IPsec) or Internet Key Exchange (IKE) policy was added and the configuration file was updated.

BCMG-1003**Message**

An IPsec/IKE policy was deleted.

Message Type

AUDIT | LOG

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that an Internet Protocol Security (IPsec) or Internet Key Exchange (IKE) policy was deleted and the configuration file was updated.

BCMG-1004**Message**

Tape Read Pipelining is being disabled slot (<slot number>) port (<user port index>) tunnel (<The configured tunnel ID (0-7)>).

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the Fabric OS version on the remote end of the tunnel does not support Tape Read Pipelining.

BCMG-1005**Message**

S<slot number>,P<user port index>(<blade index>) [OID 0x<port OID>]: <string name of ge>: port faulted due to SFP validation failure. Please check if the SFP is valid for the configuration.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates a deteriorated small form-factor pluggable (SFP) transceiver, an incompatible SFP transceiver pair, or a faulty cable between the peer ports.

Recommended Action

Verify that compatible SFP transceivers are used on the peer ports (execute the `sfpShow` command on each side to verify a matched pair), that the SFP transceivers have not deteriorated, and that the Fibre Channel cable is not faulty. Replace the SFP transceivers or the cable if necessary.

BL Messages

BL module error message.

BL-1000

Message

Initializing ports...

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the switch has started initializing the ports.

BL-1001

Message

Port initialization completed.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the switch has completed initializing the ports.

BL-1002**Message**

Init Failed: slot <slot number> DISABLED because internal ports were not ONLINE, <list of internal port number not ONLINE>.

Message Type

FFDC | LOG

Message Severity

CRITICAL

Probable Cause

Indicates that the blade initiation failed because one or more of the internal ports were not online. The blade is faulted.

Recommended Action

Make sure that the blade is seated correctly.

If the blade is seated correctly, execute the `diagPost` command to make sure that power-on self-test (POST) is enabled; then power-cycle the blade using the `slotPowerOff` and `slotPowerOn` commands or have the blade's ejector switch cycled to run POST and verify that the blade does not have any hardware problems.

Additional blade fault messages precede and follow this error, providing more information. Refer to other error messages for the recommended action.

If the message persists, replace the blade.

BL-1003**Message**

Faulting blade in slot <slot number>.

Message Type

FFDC | LOG

Message Severity

CRITICAL

Probable Cause

Indicates a faulty blade in the specified slot.

Recommended Action

Make sure that the blade is seated correctly.

If the blade is seated correctly, execute the `diagPost` command to make sure that power-on self-test (POST) is enabled; then power-cycle the blade using the `slotPowerOff` and `slotPowerOn` commands or have the blade's ejector switch cycled to run POST and verify that the blade does not have any hardware problems.

If the message persists, replace the blade.

BL-1004**Message**

Suppressing blade fault in slot <slot number>.

Message Type

FFDC | LOG

Message Severity

CRITICAL

Probable Cause

Indicates that the specified blade experienced a failure but was not faulted due to a user setting.

Recommended Action

Execute the `diagPost` command to make sure that power-on self-test (POST) is enabled; then power-cycle the blade using the `slotPowerOff` and `slotPowerOn` commands or have the blade's ejector switch cycled to run POST and verify that the blade does not have any hardware problems.

If the message persists, replace the blade.

BL-1006**Message**

Blade <slot number> NOT faulted. Peer blade <slot number> experienced abrupt failure.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the errors (mostly synchronization errors) on the specified blade are harmless. Probably, the standby control processor (CP) blade that is connected to the active CP blade has experienced transitory problems.

Recommended Action

Execute the `haShow` command to verify that the standby CP is healthy. If the problem persists, remove and reinstall the faulty blade.

If the standby CP was removed or faulted by user intervention, no action is required.

BL-1007**Message**

blade #<blade number>: blade state is inconsistent with EM. bl_cflags 0x<blade control flags>, slot_on <slot_on flag>, slot_off <slot_off flag>, faulty <faulty flag>, status <blade status>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that a failover occurred while a blade was initializing on the previously active control processor (CP).

Recommended Action

No action is required. The blade is reinitialized. Because reinitializing a blade is a disruptive operation and can stop I/O traffic, you may need to stop and restart the traffic during this process.

BL-1008**Message**

Slot <slot number> control-plane failure. Expected value: 0x<value 1>, Actual: 0x<value 2>.

Message Type

FFDC | LOG

Message Severity

CRITICAL

Probable Cause

Indicates that the blade has experienced a hardware failure or was removed without following the recommended removal procedure.

Recommended Action

Make sure that the blade is seated correctly.

If the blade is seated correctly, execute the `diagPost` command to make sure that power-on self-test (POST) is enabled; then power-cycle the blade using the `slotPowerOff` and `slotPowerOn` commands or have the blade's ejector switch cycled to run POST and verify that the blade does not have any hardware problems.

If the message persists, replace the blade.

BL-1009

Message

Blade in slot <slot number> timed out initializing the chips.

Message Type

FFDC | LOG

Message Severity

CRITICAL

Probable Cause

Indicates that the blade has failed to initialize the application-specific integrated circuit (ASIC) chips.

Recommended Action

Make sure that the blade is seated correctly.

If the blade is seated correctly, execute the `diagPost` command to make sure that power-on self-test (POST) is enabled; then power-cycle the blade using the `slotPowerOff` and `slotPowerOn` commands or have the blade's ejector switch cycled to run POST and verify that the blade does not have any hardware problems.

If the message persists, replace the blade.

BL-1010

Message

Blade in slot <slot number> inconsistent with the hardware settings.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that a failover occurred while some hardware changes (such as changing the domain ID) were being made on the previously active control processor (CP).

Recommended Action

No action is required. This blade has been reinitialized. Because reinitializing a blade is a disruptive operation and can stop I/O traffic, you may need to stop and restart the traffic during this process.

BL-1011**Message**

Busy with emb-port int. for chip <chip number> in minis <minis number> on blade <slot number>, chip int. is disabled. interrupt status=0x<interrupt status>.

Message Type

FFDC | LOG

Message Severity

CRITICAL

Probable Cause

Indicates that too many interrupts in the embedded port caused the specified chip to be disabled. The probable cause is too many abnormal frames; the chip is disabled to prevent the control processor (CP) from becoming too busy.

Recommended Action

Make sure to capture the console output during this process.

Check for a faulty cable, small form-factor pluggable (SFP) transceiver, or device attached to the specified port.

On a bladed switch, execute the `diagPost` command to make sure that power-on self-test (POST) is enabled; then power-cycle the blade using the `slotPowerOff` and `slotPowerOn` commands or have the blade's ejector switch cycled to run POST and verify that the blade does not have any hardware problems.

On a nonbladed switch, reboot or power cycle the switch.

If the message persists, replace the blade or the (nonbladed) switch.

BL-1012**Message**

bport <port number> port int. is disabled. status=0x<interrupt status> Port <port number> will be re-enabled in 1 minute.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the port generated an excessive number of interrupts that may prove unrecoverable to the switch operation. The port is disabled to prevent the control processor (CP) from becoming too busy. The bport is the blade port; this number may not correspond to a user port number.

Recommended Action

Make sure to capture the console output during this process.

Check for a faulty cable, small form-factor pluggable (SFP) transceiver, or device attached to the specified port.

On a bladed switch, run the `slotPowerOff` and `slotPowerOn` commands to power-cycle the blade.

On a nonbladed switch, reboot or power-cycle the switch.

If the message persists, replace the blade or the (nonbladed) switch.

BL-1013**Message**

bport <port number> port is faulted. status=0x<interrupt status> Port <port number> will be re-enabled in 1 minute.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the port generated an excessive number of interrupts that may prove fatal to the switch operation. The port is disabled to prevent the control processor (CP) from becoming too busy. The bport number displayed in the message is the blade port; this number may not correspond to a user port number.

Recommended Action

Make sure to capture the console output during this process.

Check for a faulty cable, small form-factor pluggable (SFP) transceiver, or device attached to the specified port.

On a bladed switch, run the `slotPowerOff` and `slotPowerOn` commands to power-cycle the blade.

On a nonbladed switch, reboot or power-cycle the switch.

If the message persists, replace the blade.

BL-1014**Message**

bport <port number> port int. is disabled. status=0x<interrupt status>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the port generated an excessive number of interrupts that may prove fatal to the switch operation. The port is disabled to prevent the control processor (CP) from becoming too busy. The bport number displayed in the message is the blade port; this number may not correspond to a user port number.

Recommended Action

Make sure to capture the console output during this process.

On a bladed switch, execute the `diagPost` command to make sure that power-on self-test (POST) is enabled; then power-cycle the blade using the `slotPowerOff` and `slotPowerOn` commands or have the blade's ejector switch cycled to run POST and verify that the blade does not have any hardware problems.

On a nonbladed switch, execute the `reboot` command to restart the switch.

If there is a hardware error, if `slotPowerOff` or `slotPowerOn` fails on the bladed switch, or if errors are encountered again, replace the blade or the (nonbladed) switch.

BL-1015**Message**

bport <port number> port is faulted. status=0x<interrupt status>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the port generated an excessive number of interrupts that may prove fatal to the switch operation. The port is disabled to prevent the control processor (CP) from becoming too busy. The bport number displayed in the message is the blade port; this number may not correspond to a user port number.

Recommended Action

Make sure to capture the console output during this process.

On a bladed switch, execute the `diagPost` command to make sure that power-on self-test (POST) is enabled; then power-cycle the blade using the `slotPowerOff` and `slotPowerOn` commands or have the blade's ejector switch cycled to run POST and verify that the blade does not have any hardware problems.

On a nonbladed switch, execute the `reboot` command to restart the switch.

If there is a hardware error, if `slotPowerOff` or if `slotPowerOn` fails on the bladed switch, or errors are encountered again, replace the blade or the (nonbladed) switch.

BL-1016

Message

Blade port <port number> in slot <slot number> failed to enable.

Message Type

FFDC | LOG

Message Severity

CRITICAL

Probable Cause

Indicates that the specified blade port could not be enabled.

Recommended Action

Make sure that the blade is seated correctly.

If the blade is seated correctly, execute the `diagPost` command to make sure that power-on self-test (POST) is enabled; then power-cycle the blade using the `slotPowerOff` and `slotPowerOn` commands or have the blade's ejector switch cycled to run POST and verify that the blade does not have any hardware problems.

If the message persists, replace the blade.

BL-1017

Message

Slot <slot number> Initializing...

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the slot has started initializing the ports.

BL-1018

Message

Slot <slot number> Initialization completed.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the slot has completed initializing the ports.

BL-1019**Message**

Slot <Slot number>, retry <Retry Number>, internal port retry initialization, <List of internal ports retrying initialization>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the slot had internal ports that are not online. Initiated a retry on the ports that failed to go online.

BL-1020**Message**

Switch timed out initializing the chips.

Message Type

LOG | FFDC

Message Severity

CRITICAL

Probable Cause

Indicates that the switch has failed to initialize the application-specific integrated circuit (ASIC) chips.

Recommended Action

Reboot or power-cycle the switch. If the message persists, replace the switch.

BL-1021

Message

Retry <Retry Number>, internal port retry initialization, <List of internal ports retrying initialization>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the switch had internal ports that are not online. Initiated a retry on the ports that failed to go online.

BL-1022

Message

Init Failed: Switch DISABLED because internal ports were not ONLINE, <list of internal port number not ONLINE>.

Message Type

LOG

Message Severity

CRITICAL

Probable Cause

Indicates that the switch initiation failed because one or more of the internal ports were not online. The switch is faulted.

Recommended Action

Reboot or power-cycle the switch.

Additional fault messages precede and follow this error, providing more information. Refer to other error messages for the recommended action.

If the message persists, replace the switch.

BL-1023

Message

Blade in slot <slot number> was reset before blade init completed. As a result the blade is faulted.

Message Type

LOG

Message Severity

CRITICAL

Probable Cause

Indicates that the blade was reset before the initialization completed.

Recommended Action

Reboot or power-cycle the blade using the `slotPowerOff` and `slotPowerOn` commands.

If the message persists, replace the blade.

BL-1024**Message**

All ports on the blade in slot <slot number> will be reset as part of the firmware upgrade.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that a recent firmware upgrade caused the blade firmware to be upgraded and resulted in a cold upgrade. As part of the upgrade, all datapath elements were reset.

BL-1025**Message**

All GigE/FCIP/Virtualization/FC Fastwrite ports on the blade in slot <slot number> will be reset as part of the firmware upgrade.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that a recent firmware upgrade caused the blade's firmware to be upgraded and resulted in a cold upgrade. As part of the upgrade, all the Gigabit Ethernet, Fibre Channel over IP (FCIP), virtualization data elements, and FC Fastwrite ports were reset.

BL-1026

Message

Internal port offline during warm recovery, state <port state> (0x<port ID>).

Message Type

LOG

Message Severity

CRITICAL

Probable Cause

Indicates that an internal port went offline during warm recovery of the switch. The switch will reboot and start a cold recovery.

Recommended Action

Execute the `supportSave` command and then reboot switch. If the problem persists, replace the switch.

BL-1027

Message

Blade in slot <slot number> faulted, boot failed; status 0x<boot status> 0x<1250 0 boot status> 0x<1250 1 boot status>.

Message Type

LOG

Message Severity

CRITICAL

Probable Cause

Indicates that the blade failed to boot properly.

Recommended Action

Reboot or power-cycle the blade using the `slotPowerOff` and `slotPowerOn` commands.

If the message persists, replace the blade.

BL-1028

Message

Switch faulted; internal processor was reset before switch init completed.

Message Type

LOG

Message Severity

CRITICAL

Probable Cause

Indicates that the switch internal processor was reset before the initialization completed.

Recommended Action

Reboot or power-cycle the switch using the `slotPowerOff` and `slotPowerOn` commands.

If the message persists, replace the switch.

BL-1029**Message**

All ports on the switch will be reset as part of the firmware upgrade.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that a recent firmware upgrade caused the switch internal processor firmware to be upgraded and resulted in a cold upgrade. As part of the upgrade, all the datapath elements were reset.

BL-1030**Message**

All GigE/FCIP/Virtualization/FC Fastwrite ports on the switch will be reset as part of the firmware upgrade.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that a recent firmware upgrade caused the switch internal processor firmware to be upgraded and resulted in a cold upgrade. As part of the upgrade, all Gigabit Ethernet, Fibre Channel over IP (FCIP), virtualization data elements, and FC Fastwrite ports were reset.

BL-1031**Message**

Link timeout in internal port (slot <slot number>, port <port number>) resulted in blade fault. Use slotpoweroff/slotpoweron to recover the blade.

Message Type

LOG

Message Severity

CRITICAL

Probable Cause

Indicates that the link timeout occurred in one of the back-end internal ports.

Recommended Action

Power-cycle the blade using the `slotPowerOff` and `slotPowerOn` commands.

BL-1032**Message**

(slot <slot number>,bitmap 0x<object control flags(bitmap)>) ports never came up ONLINE (reason <reason for port disable>, state <status of the blade>). Disabling slot.

Message Type

LOG

Message Severity

CRITICAL

Probable Cause

Indicates that back-end (nonuser) ports have not come online within the time limit.

Recommended Action

Execute the `diagPost` command to make sure that power-on self-test (POST) is enabled; then power-cycle the blade using the `slotPowerOff` and `slotPowerOn` commands or have the blade's ejector switch cycled to run POST and verify that the blade does not have any hardware problems.

If the message persists, replace the blade.

BL-1033

Message

(slot <slot number>,bitmap 0x<object control flags(bitmap)>) No disable acknowledgment from ports (state <status of the blade>). Disabling slot.

Message Type

LOG

Message Severity

CRITICAL

Probable Cause

Indicates that the system has timed out waiting for the disable messages from the user ports after disabling the ports.

Recommended Action

Execute the `diagPost` command to make sure that power-on self-test (POST) is enabled; then power-cycle the blade using the `slotPowerOff` and `slotPowerOn` commands or have the blade's ejector switch cycled to run POST and verify that the blade does not have any hardware problems.

If the message persists, replace the blade.

BL-1034

Message

Slot <slot number> FC Initialization completed.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the slot has completed initializing the Fibre Channel (FC) ports.

BL-1035

Message

Slot <slot number> iSCSI port <iscsi port number> Initialization completed.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the slot has completed initializing the specified iSCSI port.

BL-1036**Message**

Faulting 8G blade in slot = <slot number> due to incompatible stag mode. All EX/VEX ports must be disabled in order to enable the 8G blade in the chassis.

Message Type

LOG

Message Severity

CRITICAL

Probable Cause

Indicates that the 8Gb/s blade with legacy mode (EX_Port having stag) will be disabled.

Recommended Action

Disable all EX_Ports and VEX_Ports and execute the `slotPowerOff` or `slotPowerOn` commands on the 8Gb/s blade. All EX_Ports and VEX_Ports can be re-enabled.

BL-1037**Message**

Faulting chip in slot = <slot number>, miniS = <miniS number>,port = <port number> due to BE/BI port fault.

Message Type

LOG

Message Severity

CRITICAL

Probable Cause

Indicates that all ports on the chip have been disabled due to a fault on the chip.

Recommended Action

Make sure that the blade is seated correctly.

If the blade is seated correctly, execute the `diagPost` command to make sure that power-on self-test (POST) is enabled; then power-cycle the blade using the `slotPowerOff` and `slotPowerOn` commands or have the blade's ejector switch cycled to run POST and verify that the blade does not have any hardware problems.

Additional blade fault messages precede and follow this error, providing more information. Refer to other error messages for the recommended action.

If the message persists, replace the blade.

BL-1038

Message

Inconsistent FPGA image version detected, please reboot the switch for recovery.

Message Type

LOG

Message Severity

CRITICAL

Probable Cause

Indicates that the field-programmable gate array (FPGA) image version is incompatible with the software version.

Recommended Action

Reboot the switch. If the message persists, replace the switch.

BL-1039

Message

Inconsistent FPGA image version detected, faulting the blade in slot <slot number>.

Message Type

LOG

Message Severity

CRITICAL

Probable Cause

Indicates that the field-programmable gate array (FPGA) image version is incompatible with the software version.

Recommended Action

Power-cycle the blade using the `slotPowerOff` and `slotPowerOn` commands.

If the message persists, replace the blade.

BL-1040

Message

Inconsistent FPGA image version detected for blade in slot <slot number>. Current FPGA ver=0x<current FPGA version major>_<current FPGA version minor> Upgrade to FPGA ver=0x<new FPGA version major>_<new FPGA version minor>

Message Type

LOG

Message Severity

CRITICAL

Probable Cause

Indicates that the field-programmable gate array (FPGA) image version is incompatible with the software version.

Recommended Action

Power-cycle the blade using the `slotPowerOff` and `slotPowerOn` commands.

If the message persists, replace the blade.

BL-1041

Message

Dynamic area mode is enabled on default switch, Faulting the blade w/ ID <Blade ID of blade that has the mini SFP+ that does not support it> in slot <slot number> as it does not support this mode.

Message Type

LOG

Message Severity

CRITICAL

Probable Cause

Indicates that the blade does not support dynamic area mode on the default switch.

Recommended Action

Turn off the dynamic area mode using the `configure` command.

BL-1045

Message

mini SFP+ (SN: <mini SFP+ serial number>) is only supported in certain high port count blades, not blade in slot <slot number of blade that has the mini SFP+> w/ ID <Blade ID of blade that has the mini SFP+ that does not support it>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that mini-SFP+ is supported only by a certain type of blade (FC8-64), but it can be inserted in other blades.

Recommended Action

Replace the mini-SFP+ with an SFP or SFP+.

BL-1046

Message

<Slot number of blade that has the SFP> error on SFP in Slot <Port number into which the SFP is inserted>/Port <The type of error "checksum" or "data access" for general problems accessing the i2c accessible data> (<A detailed error code>). Try reseating or replacing it.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the checksum in an area on the small form-factor pluggable (SFP) transceiver does not match with the computed value, or there is problem accessing the data.

Recommended Action

Reseat the SFP transceiver. If the problem persists, replace the SFP transceiver.

BL-1047

Message

Buffer optimized mode is turned <buffer optimized mode> for slot <slot number>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the buffer optimized mode is changed for the specified slot.

BL-1048**Message**

FCoE Blade in slot <Slot> failed because the Interop mode is enabled on the switch.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the interop mode is turned on in the default switch while powering on the FCoE blade.

Recommended Action

Disable the interop mode using the `interopmode` command; then execute the `slotPowerOff` and `slotPowerOn` commands on the FCoE blade.

BL-1049**Message**

Serdestunemode: <serdestuning mode>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the SerDes tuning mode has changed for the slot.

BL-1050

Message

Incompatible Blade Processor FPGA version with current FOS firmware in slot=<slot number> on FX8-24. Contact support for upgrade instructions.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the blade processor field-programmable gate array (FPGA) version with current Fabric OS firmware is incompatible on the FX8-24 blade.

Recommended Action

Contact your switch service provider for upgrade instructions.

BL-1052

Message

Link Reset threshold exceeded in the internal port (slot <slot number>, port <port number>). No core blade has been faulted because it has only one active core blade.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the internal port in the core blade exceeded the link reset threshold level. Faulting the peer edge blade because there is only one active core blade.

Recommended Action

Replace the core blade.

BL-1053

Message

Invalid E_Port credits <credits> configured for slot <slot number>, port <port number>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that invalid E_Port credits are configured. The old credit model will be retained.

Recommended Action

Disable the E_Port credits using the `portcfgportcredits --disable` command.

BL-1054**Message**

QSFP (SN: <QSFP serial number>) is not supported on blade in slot <slot number of blade that has the QSFP> with ID <Blade ID of blade that has the QSFP that does not support it>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the current quad small form-factor pluggable (QSFP) is not supported by this particular type of blade (core or port), but it can be inserted in other blades. Core blades and port blades have their own supported versions of QSFPs.

Recommended Action

Replace the QSFP with one that is compatible with the blade.

BL-1055**Message**

The octet mode of user port (<Port Number>) in slot:<Slot Number of blade that has the QSFP>, blade ID <Blade ID of blade that has the QSFP that does not support it> is not supported.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the quad small form-factor pluggable (QSFP) supports only octet combo 1. If the port is configured in the other two modes (2 and 3), there is a mismatch in capabilities.

Recommended Action

Set the correct octet combo by using the `portCfgOctetSpeedCombo` command.

BL-1056**Message**

Tunable SFP user port (<Port Number>) in slot:<Slot Number of blade that has the TSFP>, blade ID <Blade ID of blade that has the TSFP that does not support it> detected with not a valid channel <Channel Number> configured. Configure valid channel range 1-102.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the user port is not configured with a valid tunable small form-factor pluggable (TSFP) channel ID. The valid range is 1 through 102.

Recommended Action

Set the correct channel by using the `portcfgge` command.

BL-1057**Message**

FIPS failure detected, blade <blade instance> will be faulted.

Message Type

LOG

Message Severity

CRITICAL

Probable Cause

Indicates that Federal Information Protection Standard (FIPS) failure is detected in one or more chips on the switch.

Recommended Action

Reboot or power-cycle the switch.

BL-1058

Message

Chip <chip instance> Restarted on BP slot <blade instance>

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the data processor (DP) has detected a PCI Express (PCIE) error.

BL-1061

Message

port speed(<port speed>G) and sfp speed(<sfp speed>G) mismatch in port(ge<port number>) slot number(<slot number>).Insert sfp matching port speed.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the port speed and the SFP speed do not match.

Recommended Action

Insert an SFP that matches the port speed.

BL-1062

Message

Unsupported sfp present in port(ge<ge port number>) in slot(<slot number>).

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that an unsupported SFP is present.

Recommended Action

Insert a supported SFP.

BL-1063**Message**

Port <User port number> has 16G QSFP and AN speed configuration is not supported.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the port number is configured for AN and installed with a 16G quad small form-factor pluggable (QSFP) in a X6 chassis.

Recommended Action

Change the port configuration to fixed 16G.

BL-1064**Message**

Chip (<Chip number>) on slot (<slot number>) going for reset to recover FPGA.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the FPGA reported errors that require a reboot to recover.

BL-1065**Message**

Internal port offline during warm recovery, state <port state> bl_cflags 0x<blade control flags> (0x<port ID>).

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that an internal port went offline before HA failover.

Recommended Action

Execute slotpoweroff-on to recover.

BL-1066**Message**

port speed(<port speed>G) and sfp speed(<sfp speed as string>) mismatch in port(ge<port number>) slot number(<slot number>).Insert sfp matching port speed.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the port speed and the SFP speed do not match.

Recommended Action

Insert an SFP that matches the port speed.

BL-1080**Message**

User port (<Port Number>) in slot:<Slot Number of blade that has the non qualified optic> (blade ID <Blade ID of blade that has the invalid SFP/QSFP module>) faulted due to detection of non qualified optic.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that a nonqualified optic was detected and shut off to prevent unexpected behavior.

Recommended Action

Replace with an officially supported optic.

BL-1081**Message**

Current sysfpga version is (0x<current sysfpga version>).Please upgrade to latest sysfpga version(0x<latest sysfpga version>).

Message Type

LOG | FFDC

Message Severity

ERROR

Probable Cause

Indicates that the current sysfpga version is not the latest.

Recommended Action

Upgrade to the latest sysfpga version.

BL-1082**Message**

media <partno> port <port> has temperature <temperature> above the limit.

Message Type

LOG

Message Severity

ERROR

Probable Cause

The optic temperature is above the limit

Recommended Action

Check the optic and the fans

BL-1083

Message

Slot <Slot> Blade ID 0x<Blade ID> Ver 0x<printf> has port SerDes data available in FRU SEEPROM.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates new SerDes data is available for some of the ports in the slot.

BL-1084

Message

Optical Module reset detected on slot <Slot> port <Port number> MCU version 0x<Current MCU version>(0x<Saved MCU version>) reset-count <Current reset counter>(<Saved reset counter>) reset-reason 0x<Current reset reason>(0x<Saved reset reason>).

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates the Optical Module on this port has undergone a reset and FOS Software will initiate a recovery.

BL-1085

Message

Optical Module reset recovery <action taken on the port> on slot <Slot> port <Port number>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates the Optical Module recovery status. Frames in transit will be dropped during recovery.

BL-1086**Message**

A delay in HA warm recovery on the Active CP can cause the ASSERT on the Standby CP.

Message Type

LOG

Message Severity

WARNING

Probable Cause

When the active CP takes longer during HA warm recovery, it can pause the bring-up of the standby CP processes. The pause prevents ASIC information from being initialized. Eventually, the delay/pause times out and the standby CP continues bring-up. But, since the ASIC information is not ready, the standby CP hits an ASSERT condition and reboots. This RASLOG is intended to make the debugging of such ASSERTs easier by putting the focus on the active CP instead of the standby CP.

Recommended Action

On both the active CP and standby CP, collect the /var/log/hasm.log* files and the output from the **hadump** command to help determine the reason for the delay in warm recovery to avoid future ASSERT conditions. Examples of causes for the delay include: a daemon crash on the active CP; out of order updates to the standby CP; pushing invalid data to the standby CP.

BL-1087**Message**

FPGA in slot <Slot number> should be upgraded to support the Gen7 ICL QSFP for blade ID <Blade ID of blade>.

Message Type

LOG

Message Severity

CRITICAL

Probable Cause

The blade is running an FPGA version that does not support Gen7 ICL QSFP.

Recommended Action

Run **fpgaupgrade --slot slot_num** command in order to upgrade the FPGA to the latest version.

BLS Messages

Fibre Channel over IP port configuration messages over the Brocade 7800 and FX8-24 blade.

BLS-1000

Message

<command name> of GE <port number> failed. Please retry the command. Data: inst=<ASIC instance> st=<ASIC initializing state> rsn=<reason code> fn=<message function> oid=<ASIC ID>.

Message Type

LOG | FFDC

Message Severity

ERROR

Probable Cause

Indicates that the hardware is not responding to a command request, possibly because it is busy.

Recommended Action

Retry the command.

BLS-1001

Message

FIPS <FIPS Test Name> failed; algo=<algorithm code> type=<algorithm type> slot=<Slot Number>.

Message Type

LOG | FFDC

Message Severity

CRITICAL

Probable Cause

Indicates that a Federal Information Protection Standard (FIPS) failure has occurred and requires faulting the blade or switch.

Recommended Action

Retry the command.

BLS-1002

Message

An IPsec/IKE policy was added.

Message Type

AUDIT | LOG

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that an Internet Protocol Security (IPsec) or Internet Key Exchange (IKE) policy was added and the configuration file was updated.

BLS-1003

Message

An IPsec/IKE policy was deleted.

Message Type

AUDIT | LOG

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that an Internet Protocol Security (IPsec) or Internet Key Exchange (IKE) policy was deleted and the configuration file was updated.

BLS-1004

Message

Tape Read Pipelining is being disabled slot (<slot number>) port (<user port index>) tunnel (<The configured tunnel ID (0-7)>).

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the Fabric OS version on the remote end of the tunnel does not support Tape Read Pipelining.

BLS-1005**Message**

S<slot number>,P<user port index>(<blade index>) [OID 0x<port OID>]: <string name of ge>: port faulted due to SFP validation failure. Please check if the SFP is valid for the configuration.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates a deteriorated small form-factor pluggable (SFP) transceiver, an incompatible SFP transceiver pair, or a faulty cable between the peer ports.

Recommended Action

Verify that compatible SFP transceivers are used on the peer ports, that the transceivers have not deteriorated, and that the Fibre Channel cable is not faulty. Replace the SFP transceivers or the cable if necessary.

BM Messages

Blade management error messages.

BM-1001**Message**

BM protocol version <Protocol version> in slot <Slot number>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the firmware running on the control processor (CP) cannot communicate with the application processor (AP) blade in the indicated slot and determine the AP blade's firmware version. The reason can be one of the following:

- The CP blade is running a later version of firmware than the AP blade.
- The CP blade is running an earlier version of firmware than the AP blade.

Recommended Action

The problem can be corrected by changing the firmware version on either the CP or on the AP blade. You can modify the firmware version on the CP blade by using the `firmwareDownload` command. Refer to the release notes to determine whether a nondisruptive firmware download is supported between the revisions. Because the AP and CP blades cannot communicate, it is not possible to load new firmware on the AP blade. If necessary, send the AP blade back to the factory for a firmware update.

BM-1002**Message**

Connection established between CP and blade in slot <Slot number>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the control processor (CP) has established a connection to the blade processor (BP) and can communicate.

BM-1003**Message**

Failed to establish connection between CP and blade in slot <Slot number>. Faulting blade.

Message Type

LOG | FFDC

Message Severity

WARNING

Probable Cause

Indicates that the control processor (CP) could not establish a connection to the blade processor (BP) to communicate.

Recommended Action

Execute the `slotPowerOff` and `slotPowerOn` commands or reseal the affected blade.

BM-1004

Message

Blade firmware <Blade firmware> on slot <Slot> is not consistent with system firmware <System firmware>. Auto-leveling blade firmware to match system firmware.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the policy of the specified blade is to auto-level the blade firmware to the system firmware. This may be due to one of the following reasons:

- The blade firmware was detected to be different from the control processor (CP) firmware due to a firmware upgrade.
- The blade was recently inserted and had a different version of the firmware loaded.

Recommended Action

No action is required. The blade will automatically download the updated firmware.

BM-1005

Message

FirmwareDownload timed-out for blade in slot <Slot>. Faulting blade.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the `firmwareDownload` command failed for the blade in the specified slot.

Recommended Action

Execute the `slotPowerOff` and `slotPowerOn` commands or reseal the affected blade.

BM-1006

Message

Blade is not configured. Persistently disabling all ports for blade in slot <Slot number>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the policy of the specified blade is set to persistently disable all ports the first time that the blade is detected. The message indicates either of the following:

- The blade was detected in this slot for the first time.
- The blade was configured under a different mode.

Recommended Action

Configure the blade so that it will persistently enable the ports.

BM-1007**Message**

If set, clear EX/VEX/FC Fastwrite configuration for all ports for blade in slot <Slot number>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the specified blade was detected for the first time after an FR4-18i was previously configured in the same slot. The new blade requires the specified port configurations to be cleared.

Recommended Action

No action is required. The blade ports are cleared automatically.

BM-1008**Message**

Download of blade firmware failed for blade in slot <slot>. Reissue firmwaredownload to recover.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the automatic firmware upgrade on the blade failed because the blade firmware version was detected to be different from the control processor (CP) firmware version.

Recommended Action

Execute the `firmwareDownload` command to recover the blade.

BM-1009**Message**

FirmwareDownload timed-out for application processor. Faulting switch.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the firmware download on the application processor (AP) blade failed.

Recommended Action

Execute the `slotPowerOff` and `slotPowerOn` commands or reseal the affected blade.

BM-1010**Message**

Resetting port configuration and linkcost for all ports for blade in slot <Slot number>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the specified blade was detected for the first time after an FC10-6 was previously configured in the same slot. The new blade requires resetting the port configuration and link cost.

Recommended Action

No action is required. The blade ports are cleared automatically.

BM-1053**Message**

Failed to establish connection between CP and Application Processor. Faulting switch.

Message Type

LOG | FFDC

Message Severity

WARNING

Probable Cause

Indicates that the control processor (CP) could not establish a connection with the application processor (AP) to communicate.

Recommended Action

Execute the `slotPowerOff` and `slotPowerOn` commands or reseal the affected blade.

BM-1054**Message**

AP firmware <Blade firmware> is not consistent with system firmware <System firmware>. Auto-leveling AP firmware to match system firmware.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the policy of the specified blade is set to auto-level the blade firmware to the system firmware. This may be due to one of the following reasons:

- The blade firmware was detected to be different from the control processor (CP) firmware due to a firmware upgrade.
- The blade was recently inserted and had a different version of the firmware loaded.

Recommended Action

No action is required. The blade will automatically download the updated firmware.

BM-1055

Message

Firmware download timed-out for AP. Faulting switch.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the firmware download on the application processor (AP) blade has failed.

Recommended Action

Execute the `slotPowerOff` and `slotPowerOn` commands or reseal the affected blade.

BM-1056

Message

AP is not configured. Persistently disabling all ports on the switch.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the policy of the specified switch is to persistently disable all ports the first time the AP is detected. This may be caused by one of the following reasons:

- The AP was detected for the first time on this switch.
- The switch was configured under a different mode.

Recommended Action

Configure the switch to persistently enable all ports.

BM-1058

Message

Download of AP firmware failed for the switch. Reissue firmwaredownload to recover.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the automatic firmware upgrade on the application processor (AP) failed because the firmware version running on the AP was detected to be different from the system firmware.

Recommended Action

Execute the `firmwareDownload` command to recover the AP.

C4 Messages

C4 module error messages.

C4-1001

Message

S<slot number>,P<port number>(Bp<blade port number>) user_idx:<User port index> [PID 0x<24 bit FC address>] faulted due to invalid SFP, conflicting speed or laser fault. <error message>

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates a deteriorated small form-factor pluggable (SFP) transceiver, an incompatible SFP transceiver pair, or a faulty cable between the peer ports.

Recommended Action

Verify that compatible SFP transceivers are used on the peer ports, that the SFP transceivers have not deteriorated, and that the Fibre Channel cable is not faulty. Replace the SFP transceivers or the cable if necessary.

C4-1002

Message

Port <port number> chip failed due to an internal error.

Message Type

LOG | FFDC

Message Severity

ERROR

Probable Cause

Indicates an internal error. All ports on the blade or switch will be disrupted.

Recommended Action

To recover a bladed system, execute the `slotPowerOff` and `slotPowerOn` commands on the blade. To recover a nonbladed system, execute the `fastBoot` command on the switch.

C4-1004**Message**

S<slot number>,C<chip index>: Invalid DMA ch pointer, chan:<Channel number>, good_addr:0x<Good address> bad_addr:0x<Bad address>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates an internal error in the application-specific integrated circuit (ASIC) hardware that may degrade the data traffic.

Recommended Action

Reboot the system at the next customer maintenance window. If the problem persists, replace the blade.

C4-1006**Message**

S<slot number>,C<chip index>: Various non-critical hardware errors were observed: fault1:0x<fault1_cnt>, fault2:0x<fault2_cnt> thresh1:0x<threshold_used>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that some errors were found in the hardware that may or may not impact the data traffic.

Recommended Action

No action is required. Usually these errors are transient.

C4-1007**Message**

S<slot number>,P<port number>(<blade port number>): best effort QoS will be turned off at next port state change as it is not supported under this configuration.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that Quality of Service (QoS) will be turned off automatically at the next port state change because best effort QoS is no longer supported on 4Gb/s or 8Gb/s platform long-distance ports.

C4-1008**Message**

S<slot number>,P<port number>(<blade port number>): QoS overwrites portcfglongdistance vc_translation_link_init. ARB will be used on the link.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that Quality of Service (QoS) has overwritten the fill word IDLE used on the long- distance links. Arbitrated loop (ARB) will be used on the link.

C4-1009**Message**

S<slot number>,P<port number>(<blade port number>): portcfglongdistance vc_translation_link_init = 1 overwrites fill word IDLE. ARB will be used on the link.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the `portcfglongdistance vc_translation_link_init 1` command has overwritten the fill word IDLE. Arbitrated loop (ARB) will be used on the link.

C4-1010**Message**

S<slot number>,C<chip index>: Above normal hardware errors were observed: fault1:0x<fault1_cnt>, fault2:0x<fault2_cnt> thresh2:0x<threshold_used>.

Message Type

LOG

Message Severity

CRITICAL

Probable Cause

Indicates that above-normal errors were observed in the hardware that may or may not impact the data traffic.

Recommended Action

When this error is observed persistently, power-cycle the specified blade using the `slotPowerOff` and `slotPowerOn` commands. If the problem persists, replace the blade.

C4-1011**Message**

Detected a complete loss of credit on internal back-end VC: Slot <slot number>, Port <port number>(<blade port number>) vc_no=<vc number> crd(s)lost=<Credit(s) lost>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that all credits have been lost on the specified virtual channel (VC) and port.

Recommended Action

Turn on the back-end credit recovery to reset the link and recover the lost credits. If credit recovery has already been turned on, the link will be reset to recover the credits and no action is required.

C4-1012**Message**

S<slot number>,P<port number>(<blade port number>): Link Timeout on internal port ftx=<frame transmitted> tov=<real timeout value> (><expected timeout value>) vc_no=<vc number> crd(s)lost=<Credit(s) lost> complete_loss:<Complete credit loss>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that one or more credits have been lost on a back-end port, and that there has been no traffic on that port for two seconds.

Recommended Action

Turn on the back-end credit recovery to reset the link and recover the lost credits. If credit recovery has already been turned on, the link will be reset to recover the credits and no action is required.

C4-1013**Message**

Multi RDY/Frame Loss detected on internal port of Slot <slot number>, Port <port number>(<blade port number>) m_rdy(0x<Multiple Credit(s) Lost>)/m_frame(0x<Multiple Frame(s) Lost>).

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that wait cycles to recover the lost frame or credit have been exceeded on the specified port.

Recommended Action

Turn on back-end credit recovery to reset the link and recover the lost credits. If credit recovery has already been turned on, the link will be reset to recover the credits and no action is required.

C4-1014

Message

Link Reset on Port S<slot number>,P<port number>(<blade port number>) vc_no=<vc number> crd(s)lost=<Credit(s) lost> <Source of link reset > trigger.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that one or more credits were lost and that the link has been reset.

Recommended Action

When this error is observed persistently on a back-end link, power-cycle the specified blade using the `slotPowerOff` and `slotPowerOn` commands. If the problem persists, replace the blade. When this error is observed persistently on a user port, check the physical layer errors on this port and peer port using `portStatsShow` command. If there are some physical layer errors, change the small form-factor pluggable (SFP) transceiver or the cable on the port and peer port to which this port is connected.

C4-1015

Message

Port re-initialized due to Link Reset failure on internal Port S<slot number>,P<port number>(<blade port number>).

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the specified port has re-initialized due to a link reset failure.

Recommended Action

When this error is observed persistently, power-cycle the specified blade using the `slotPowerOff` and `slotPowerOn` commands. If the problem persists, replace the blade.

C4-1016

Message

Port is faulted due to a port re-initialization failure on internal Port S<slot number>,P<port number>(<blade port number>) with reason <port fault reason>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the specified port failed due to port re-initialization failure.

Recommended Action

When this error is observed persistently, power-cycle the specified blade using the `slotPowerOff` and `slotPowerOn` commands. If the problem persists, replace the blade.

C4-1017

Message

Blade in Slot-<slot number> failed due to unavailability of ports in the internal trunk.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the specified blade failed because of the unavailability of the ports in the internal trunk.

Recommended Action

When this error is observed persistently, power-cycle the specified blade using the `slotPowerOff` and `slotPowerOn` commands. If the problem persists, replace the blade.

C4-1018

Message

Link reset threshold value exceeded in the link S<slot number>,P<port number>(<blade port number>).

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the specified blade has faulted because the link reset threshold value was exceeded.

Recommended Action

When this error is observed persistently, power-cycle the specified blade using the `slotPowerOff` and `slotPowerOn` commands. If the problem persists, replace the blade.

C4-1019**Message**

S<slot number>,C<chip index>: HW ASIC Chip TXQ FID parity error threshold reached type = 0x<chip error type>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that an internal error has been observed in the application-specific integrated circuit (ASIC) hardware that may degrade the data traffic.

Recommended Action

Restart the system at the next customer maintenance window.

C4-1020**Message**

S<slot number>,P<port number>(<blade port number>): Internal CRC with good EOF errors were observed, continuing monitoring. current:0x<last_crc_good_eof_cnt>, last:0x<total_crc_good_eof_cnt> thresh1:0x<threshold_used>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that some CRC errors were detected on a back-end link by the hardware. Typically applications are not affected at this low count.

C4-1023**Message**

Single RDY/Frame Loss detected and recovered on Slot <slot number>,Port <port number>(<blade port number>) rdy(0x<Credit Lost>)/frame(0x<Frame Lost>).

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that above-normal errors have been observed in the hardware that may or may not impact the data traffic.

Recommended Action

When this error is observed persistently, power-cycle the specified blade using the `slotPowerOff` and `slotPowerOn` commands. If the problem persists, replace the blade.

C4-1028**Message**

Detected excessive Link resets on the port in a second. Slot <slot number>, Port <port number>(<blade port number>).

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the port received excessive link resets from the peer port within 1 second and that exceeded the threshold.

Recommended Action

When this error is observed persistently, change the small form-factor pluggable (SFP) transceiver or the cable on the peer port to which this port is connected.

C4-1030

Message

S<slot number>,P<port number>(<blade port number>): Internal CRC with good EOF errors exceeded threshold, tuning is required. current:0x<last_crc_good_eof_cnt>, last:0x<total_crc_good_eof_cnt> thresh2:0x<threshold_used>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that some CRC errors were detected on a back-end link by the hardware; applications may be affected.

Recommended Action

If a core blade reset or auto tuning or manual tuning does not resolve the issue, replace the blade.

C4-1031

Message

LOSYNC timeout occurred on Slot <slot number>, Port <port number>(<blade port number>).

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that loss of synchronization has occurred on the BE port and that a link reset was invoked on this port by the blade driver.

C4-1032

Message

S<slot number>,P<port number>(<blade port number>): Required buffer unavailable for the port. req_buf:<required buffer> port_buf:<port buffer> unused_buf:<Unused buffer> est_buf:<Estimated buffer>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that free buffers in the chip are not sufficient to bring the port online in fully operational mode. The port may not come online or may operate in a degraded buffer mode.

Recommended Action

If one or more ports that are configured as long distance in the chip are unused, reset these ports to normal distance. If the problem persists, move the affected port to a different blade or chip.

C4-1033**Message**

S<slot number>,P<port number>(<blade port number>): FEC TTS is only supported on F_Port.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that Forward Error Correction (FEC) TTS is enabled on the specified port. The FEC TTS option is supported only on F_Ports.

Recommended Action

Disable the FEC TTS option using the `portcfgfec --disable -TTS` command.

C4-1034**Message**

S<slot number>,P<port number>(<blade port number>): FEC is Enabled but FEC is Inactive. Check peer port's FEC configurations.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that Forward Error Correction (FEC) is enabled but is inactive on the specified port.

Recommended Action

Check the local and peer port's FEC configurations using the `portcfgfec --show` command.

C4-1035**Message**

Credit Recovery disabled on Slot <slot number>, Port <port number>(<blade port number>) because of HW error.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that credit recovery logic has failed.

Recommended Action

Disable and enable the port, and if the error persists, disable credit recovery for the port.

C4-1036**Message**

Buffer sharing unfairness issue on Slot <slot number>, Port <port number>(<blade port number>).

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates buffer sharing unfairness and port starvation.

C4-1037**Message**

S<slot number>,C<chip index>: IOS Error, block 1st = 0x<Top level first error value>, intr_cause = 0x<IOS error intr cause>, ios_int_en_set = 0x<IOS intr status> single bit error <Single bit error count>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the hardware parity error has been detected in the Condor 4 Inter-network Operating System (IOS) block.

Recommended Action

IOS counters may have been corrupted; ignore IOS flow counters in the last polling cycle.

C4-1038**Message**

Slow drain device quarantine (SDDQ) or Restore action is not completed for the sid 0x<Source ID>, did 0x<Destination ID>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the Frame Transformation Block (FTB) entry has not been added.

C4-1039**Message**

S<slot number>,C<chip index>: Temperature is <current temperature>, maximum threshold is <Maximum operating temperature>. If it exceeds threshold, the unit will be shutdown.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the operating environment conditions are causing the application-specific integrated circuit (ASIC) to overheat.

Recommended Action

Make sure that the area is well ventilated and that the room temperature is within the operational range of your switch. Refer to the hardware reference manual for your switch for the operational temperature range.

C4-1040

Message

Multi RDY/Frame Loss detected on Slot <slot number>, Port <port number>(<blade port number>) m_rdy(0x<Multiple Credit(s) Lost>)/m_frame(0x<Multiple Frame(s) Lost>). Link Reset done.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that multiple credits and frames were lost on the specified port, and that the link has reset.

C4-1041

Message

Encryption block error event detected on Slot <slot number>, Port <port number>(<blade port number>), err_count:<error counter>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that encryption block errors have been detected.

Recommended Action

Disable and enable the port, and if the problem persists, replace the blade.

C4-1042

Message

Port in Slot <slot number>, Port <port number>(<blade port number>) getting faulted because of encryption block error.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the port has faulted because of encryption block errors.

Recommended Action

Disable and enable the port, and if the problem persists, replace the blade.

C4-1043**Message**

Encryption enabled Port S<slot number>,P<port number>(<blade port number>) faulted due to link initialization failure.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that an encryption-configured port failed because of a link initialization failure.

Recommended Action

Disable and enable the port, and if the problem persists, replace the blade.

C4-1044**Message**

Trunk performance impact on port (<port number>) due to high deskew value. [TRUNK_PERF:<perf> percent, Deskew:<deskew>]

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates a high deskew value on the port.

Recommended Action

Check for physical cable length differences among physical ports of the trunk. If there are cable length differences then fix them with the same cable length link. Otherwise replace the cable if the problem persists.

C4-1045**Message**

Single parity error detected in ftb statistics memory, slot <slot> index <index>

Message Type

LOG

Message Severity

INFO

Probable Cause

A parity error was detected in FTB statistics memory; a Flow Vision flow monitor may show incorrect statistics.

Recommended Action

Reset the Flow Vision flow monitor flow that is showing abnormal statistics.

C4-1046**Message**

Multiple parity errors detected in ftb statistics memory, slot <slot> indexes <index> <index> <index> <index>

Message Type

LOG

Message Severity

INFO

Probable Cause

A parity error was detected in FTB statistics memory; a Flow Vision flow monitor may show incorrect statistics.

Recommended Action

Reset the Flow Vision flow monitor flow that is showing abnormal statistics.

C4-1047

Message

Slot <slot number>, Port <port number>(<blade port number>) is getting faulted because another Encryption and Trunking configured <port type getting faulted>-port (<Already present Encryption and Trunking configured port>) is already present.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the port has faulted because another type of encryption- and trunking- configured port is already present in the chip.

Recommended Action

Disable the other type of encryption- and trunking- configured port, and enable the port that is getting the hard fault.

C4-1048

Message

S<Slot number>,C<Chip Index>: Maximum possible buffers (<Maximum possible buffers>) exceeded; total desired:<Total Number of buffers desired>; port <Port with high desired count> has high desired count:<Desired buffer count on the one port>

Message Type

LOG | FFDC

Message Severity

ERROR

Probable Cause

More buffers have been requested/desired than exist on the ASIC. This will cause traffic disruption in the fabric.

Recommended Action

If the port is a frontend port, toggle the identified port using portdisable, portenable, portcfgpersistentdisable, or portcfgpersistentenable. If that doesn't work, or if the port is a backend port, use slotpoweroff and slotpoweron on the identified blade. If this message appears again for the same blade, replace the blade.

C4-1049

Message

S<Slot number>,P<User port index>(<Blade port number>): Port faulted at <String to identify location>. Requested <Desired buffer count on the one port> buffers; ASIC buffers: current=<Total Number of buffers desired on ASIC> max=<Maximum possible buffers>

Message Type

LOG | FFDC

Message Severity

ERROR

Probable Cause

More buffers have been requested/desired than exist on the ASIC. This will cause traffic disruption in the fabric.

Recommended Action

First, collect a supportsave and contact the switch vendor for analysis. If the number of requested buffers by the port is unexpectedly large, and if the port is a frontend port, toggle the identified port using portdisable, portenable, portcfgpersistentdisable, or portcfgpersistentenable. If that doesn't work, or if the port is a backend port, use slotpoweroff and slotpoweron on the identified blade. If the number of requested buffers makes sense and the current total ASIC buffers is very close to the ASIC maximum, contact the switch vendor to analyze switch data for possible ports to toggle and the next actions to take on the switch.

C4-1050

Message

S<Slot number>,C<Chip index>: No buffers allocated to <String to specify type of port> port. Requested <Desired buffer count on the one port> buffers; ASIC buffers: current=<Total Number of buffers desired on ASIC> max=<Maximum possible buffers>

Message Type

LOG | FFDC

Message Severity

ERROR

Probable Cause

More buffers have been requested/desired than exist on the ASIC. This will cause traffic disruption in the fabric.

Recommended Action

First, take a supportsave and contact the switch vendor for analysis. If the number of requested buffers by the port is unexpectedly large, or if the number of requested buffers makes sense and the current total ASIC buffers is very close to

the ASIC maximum, contact the switch vendor to analyze switch data for possible ports to toggle and the next actions to take on the switch.

C4-1051

Message

S<Slot number>,P<User port index>(<chip index>)(C<Blade port number>): Port desired buffer mismatch. actual: <Actual desired buffer count on the port> expected: <Expected desired buffer count on the port>

Message Type

LOG | FFDC

Message Severity

ERROR

Probable Cause

The number of buffers requested by a port does not match the number of buffers this port is supposed to request.

Recommended Action

First, collect a supportsave and contact the switch vendor. If the number of requested buffers by the port is unexpectedly large, and if the port is a frontend port, toggle the identified port using portdisable, portenable, portcfgpersistentdisable, or portcfgpersistentenable. If that doesn't work, or if the port is a backend port, use slotpoweroff and slotpoweron on the identified blade.

C4-1052

Message

S<Slot number>,C<Chip index>: <String to specify type of port> port desired buffer mismatch. actual: <Actual desired buffer count on the port> expected: <Expected desired buffer count on the port>

Message Type

LOG | FFDC

Message Severity

ERROR

Probable Cause

The number of buffers requested by a port does not match the number of buffers this port is supposed to request.

Recommended Action

First, take a supportsave and contact the switch vendor for analysis. If the number of requested buffers by the port is unexpectedly large, contact the switch vendor to analyze switch data for the next actions to take on the switch.

C4-1054

Message

S<slot number>,P<port number>(<blade port number>): Media initialization fault; please reseal or replace media
rtryctr:<retries left>/<max retries > rate:<High(2)/Low rate(1)> failure:<failure code>.

Message Type

LOG | FFDC

Message Severity

ERROR

Probable Cause

A Media initialization fault occurs because the media is not seated properly or the SFP is faulty.Actions such as media plug-out/plug-in and switch power-cycle can cause this fault.

Recommended Action

Follow these steps: 1. Disable the port, and then enable it. 2. Reseat the media. 3. If reseating does not recover the module, replace the module.

C4-1055

Message

Port in Slot <slot number>, Port <port number>(<blade port number>) getting faulted with reason <port fault reason>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the port has faulted because of errors.

Recommended Action

Disable and enable the port, and if the problem persists, replace the blade.

C4-1056

Message

Chip in Slot <slot number>, Chip <chip index> getting faulted with reason <Fault reason>.

Message Type

LOG

Message Severity

CRITICAL

Probable Cause

Indicates that above-normal errors were observed in the hardware and the chip has faulted.

Recommended Action

When this error is observed persistently, power-cycle the specified blade using the `slotPowerOff` and `slotPowerOn` commands. If the problem persists, replace the blade.

C5 Messages

C5 module error messages.

C5-1001

Message

S<slot number>,P<port number>(Bp<blade port number>) user_idx:<User port index> [PID 0x<24 bit FC address>] faulted due to invalid SFP, conflicting speed or laser fault. <error message>

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates a deteriorated small form-factor pluggable (SFP) transceiver, an incompatible SFP transceiver pair, or a faulty cable between the peer ports.

Recommended Action

Verify that compatible SFP transceivers are used on the peer ports, that the SFP transceivers have not deteriorated, and that the Fibre Channel cable is not faulty. Replace the SFP transceivers or the cable if necessary.

C5-1002

Message

Port <port number> chip failed due to an internal error.

Message Type

LOG | FFDC

Message Severity

ERROR

Probable Cause

Indicates an internal error. All ports on the blade or switch will be disrupted.

Recommended Action

To recover a bladed system, execute the `slotPowerOff` and `slotPowerOn` commands on the blade. To recover a nonbladed system, execute the `fastBoot` command on the switch.

C5-1004**Message**

S<slot number>,C<chip index>: Invalid DMA ch pointer, chan:<Channel number>, good_addr:0x<Good address>
bad_addr:0x<Bad address>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates an internal error in the application-specific integrated circuit (ASIC) hardware that may degrade the data traffic.

Recommended Action

Reboot the system at the next customer maintenance window. If the problem persists, replace the blade.

C5-1006**Message**

S<slot number>,C<chip index>: Various non-critical hardware errors were observed: fault1:0x<fault1_cnt>,
fault2:0x<fault2_cnt> thresh1:0x<threshold_used>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that some errors were found in the hardware that may or may not impact the data traffic.

Recommended Action

No action is required. Usually these errors are transient.

C5-1007**Message**

S<slot number>,P<port number>(<blade port number>): best effort QoS will be turned off at next port state change as it is not supported under this configuration.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that Quality of Service (QoS) will be turned off automatically at the next port state change because best effort QoS is no longer supported on 8Gb/s platform long-distance ports.

C5-1008**Message**

S<slot number>,P<port number>(<blade port number>): QoS overwrites portcfglongdistance vc_translation_link_init. ARB will be used on the link.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that Quality of Service (QoS) has overwritten the fill word IDLE used on the long-distance links. Arbitrated loop (ARB) will be used on the link.

C5-1009**Message**

S<slot number>,P<port number>(<blade port number>): portcfglongdistance vc_translation_link_init = 1 overwrites fill word IDLE. ARB will be used on the link.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the `portcfglongdistance vc_translation_link_init 1` command has overwritten the fill word IDLE. Arbitrated loop (ARB) will be used on the link.

C5-1010**Message**

S<slot number>,C<chip index>: Above normal hardware errors were observed: fault1:0x<fault1_cnt>, fault2:0x<fault2_cnt> thresh2:0x<threshold_used>.

Message Type

LOG

Message Severity

CRITICAL

Probable Cause

Indicates that above-normal errors were observed in the hardware that may or may not impact the data traffic.

Recommended Action

When this error is observed persistently, power-cycle the specified blade using the `slotPowerOff` and `slotPowerOn` commands. If the problem persists, replace the blade.

C5-1011**Message**

Detected a complete loss of credit on internal back-end VC: Slot <slot number>, Port <port number>(<blade port number>) vc_no=<vc number> crd(s)lost=<Credit(s) lost>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that all credits have been lost on the specified virtual channel (VC) and port.

Recommended Action

Turn on back-end credit recovery to reset the link and recover the lost credits. If credit recovery has already been turned on, the link will be reset to recover the credits and no action is required.

C5-1012**Message**

S<slot number>,P<port number>(<blade port number>): Link Timeout on internal port ftx=<frame transmitted> tov=<real timeout value> (><expected timeout value>) vc_no=<vc number> crd(s)lost=<Credit(s) lost> complete_loss:<Complete credit loss>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that one or more credits have been lost on a back-end port and that there has been no traffic on that port for two seconds.

Recommended Action

Turn on back-end credit recovery to reset the link and recover the lost credits. If credit recovery has already been turned on, the link will be reset to recover the credits and no action is required.

C5-1013**Message**

Multi RDY/Frame Loss detected on internal port of Slot <slot number>, Port <port number>(<blade port number>) m_rdy(0x<Multiple Credit(s) Lost>)/m_frame(0x<Multiple Frame(s) Lost>).

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that wait cycles to recover the lost frame or credit have been exceeded on the specified port.

Recommended Action

Turn on back-end credit recovery to reset the link and recover the lost credits. If credit recovery has already been turned on, the link will be reset to recover the credits and no action is required.

C5-1014

Message

Link Reset on Port S<slot number>,P<port number>(<blade port number>) vc_no=<vc number> crd(s)lost=<Credit(s) lost> <Source of link reset > trigger.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that one or more credits were lost and that the link has been reset.

Recommended Action

When this error is observed persistently on back-end link, power-cycle the specified blade using the `slotPowerOff` and `slotPowerOn` commands. If the problem persists, replace the blade. When this error is observed persistently on a user port, check the physical layer errors on this port and peer port using `portStatsShow` command. If there are some physical layer errors, change the small form-factor pluggable (SFP) transceiver or the cable on the port and peer port to which this port is connected.

C5-1015

Message

Port re-initialized due to Link Reset failure on internal Port S<slot number>,P<port number>(<blade port number>).

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the specified port has re-initialized due to a link reset failure.

Recommended Action

When this error is observed persistently, power-cycle the specified blade using the `slotPowerOff` and `slotPowerOn` commands. If the problem persists, replace the blade.

C5-1016

Message

Port is faulted due to port re-initialization failure on internal Port S<slot number>,P<port number>(<blade port number>) with reason <port fault reason>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the specified port failed due to a port re-initialization failure.

Recommended Action

When this error is observed persistently, power-cycle the specified blade using the `slotPowerOff` and `slotPowerOn` commands. If the problem persists, replace the blade.

C5-1017

Message

Blade in Slot-<slot number> failed due to unavailability of ports in the internal trunk.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the specified blade failed because of the unavailability of the ports in the internal trunk.

Recommended Action

When this error is observed persistently, power-cycle the specified blade using the `slotPowerOff` and `slotPowerOn` commands. If the problem persists, replace the blade.

C5-1018

Message

Link reset threshold value exceeded in the link S<slot number>,P<port number>(<blade port number>).

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the specified blade has faulted because the link reset threshold value was exceeded.

Recommended Action

When this error is observed persistently, power-cycle the specified blade using the `slotPowerOff` and `slotPowerOn` commands. If the problem persists, replace the blade.

C5-1019**Message**

S<slot number>,C<chip index>: HW ASIC Chip TXQ FID parity error threshold reached type = 0x<chip error type>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that an internal error has been observed in the application-specific integrated circuit (ASIC) hardware that may degrade the data traffic.

Recommended Action

Restart the system at the next customer maintenance window.

C5-1020**Message**

S<slot number>,P<port number>(<blade port number>): Internal CRC with good EOF errors were observed, continuing monitoring. current:0x<last_crc_good_eof_cnt>, last:0x<total_crc_good_eof_cnt> thresh1:0x<threshold_used>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that some CRC errors were detected on a back-end link by the hardware. Typically applications are not affected at this low count.

C5-1023**Message**

Single RDY/Frame Loss detected and recovered on Slot <slot number>,Port <port number>(<blade port number>) rdy(0x<Credit Lost>)/frame(0x<Frame Lost>).

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that above-normal errors have been observed in the hardware that may or may not impact the data traffic.

Recommended Action

When this error is observed persistently, power-cycle the specified blade using the `slotPowerOff` and `slotPowerOn` commands. If the problem persists, replace the blade.

C5-1028**Message**

Detected excessive Link resets on the port in a second. Slot <slot number>, Port <port number>(<blade port number>).

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the port received excessive link resets from the peer port within 1 second and that exceeded the threshold.

Recommended Action

When this error is observed persistently, change the small form-factor pluggable (SFP) transceiver or the cable on the peer port to which this port is connected.

C5-1030

Message

S<slot number>,P<port number>(<blade port number>): Internal CRC with good EOF errors exceeded threshold, tuning is required. current:0x<last_crc_good_eof_cnt>, last:0x<total_crc_good_eof_cnt> thresh2:0x<threshold_used>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that some CRC errors have been detected on back-end link by hardware; applications may be affected.

Recommended Action

If a core blade reset or auto tuning or manual tuning does not resolve the issue, replace the blade.

C5-1031

Message

LOSYNC timeout occurred on Slot <slot number>, Port <port number>(<blade port number>).

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that loss of synchronization has occurred on the BE port and that a link reset was invoked on this port by the blade driver.

C5-1032

Message

S<slot number>,P<port number>(<blade port number>): Required buffer unavailable for the port. req_buf:<required buffer> port_buf:<port buffer> unused_buf:<Unused buffer> est_buf:<Estimated buffer>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that free buffers in the chip are not sufficient to bring the port online in fully operational mode. The port may not come online or may operate in a degraded buffer mode.

Recommended Action

If one or more ports that are configured as long distance in the chip are unused, reset these ports to normal distance. If the problem persists, move the affected port to a different blade or chip.

C5-1033**Message**

S<slot number>,P<port number>(<blade port number>): FEC TTS is only supported on F_Port.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that Forward Error Correction (FEC) TTS is enabled on the specified port. The FEC TTS option is supported only on F_Ports.

Recommended Action

Disable the FEC TTS option using the `portcfgfec --disable -TTS` command.

C5-1034**Message**

S<slot number>,P<port number>(<blade port number>): FEC is Enabled but FEC is Inactive. Check peer port's FEC configurations.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that Forward Error Correction (FEC) is enabled but is inactive on the specified port.

Recommended Action

Check the local and peer port's FEC configurations using the `portcfgfec --show` command.

C5-1035**Message**

Credit Recovery disabled on Slot <slot number>, Port <port number>(<blade port number>) because of HW error.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that credit recovery logic has failed.

Recommended Action

Disable and enable the port, and if the error persists, disable credit recovery for the port.

C5-1036**Message**

Buffer sharing unfairness issue on Slot <slot number>, Port <port number>(<blade port number>).

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates buffer sharing unfairness and port starvation.

C5-1037**Message**

S<slot number>,C<chip index>: DAE Error, first error top = 0x<first error top>, intr_cause = 0x<intr cause>, first_err = 0x<first error> first_err_info 0x<first error info>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that a hardware parity error has been detected in the Condor5 DAE block.

Recommended Action

DAE counters may have been corrupted; ignore DAE flow counters in the last polling cycle.

C5-1038**Message**

Slow drain device quarantine (SDDQ) or Restore action is not completed for the sid 0x<Source ID>, did 0x<Destination ID>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the Frame Transformation Block (FTB) entry has not been added.

C5-1039**Message**

S<slot number>,C<chip index>: Temperature is <current temperature>, maximum threshold is <Maximum operating temperature>. If it exceeds threshold, the unit will be shutdown.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the operating environment conditions are causing the application-specific integrated circuit (ASIC) to overheat.

Recommended Action

Make sure that the area is well ventilated and that the room temperature is within the operational range of your switch. Refer to the hardware reference manual for your switch for the operational temperature range.

C5-1040

Message

Multi RDY/Frame Loss detected on Slot <slot number>, Port <port number>(<blade port number>) m_rdy(0x<Multiple Credit(s) Lost>)/m_frame(0x<Multiple Frame(s) Lost>). Link Reset done.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that multiple credits and frames were lost on the specified port and that the link has reset.

C5-1041

Message

Encryption block error event detected on Slot <slot number>, Port <port number>(<blade port number>), err_count:<error counter>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that encryption block errors have been detected.

Recommended Action

Disable and enable the port, and if the problem persists, replace the blade.

C5-1042

Message

Port in Slot <slot number>, Port <port number>(<blade port number>) getting faulted because of encryption block error.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the port has faulted because of encryption block errors.

Recommended Action

Disable and enable the port, and if the problem persists, replace the blade.

C5-1043**Message**

Encryption enabled Port S<slot number>,P<port number>(<blade port number>) faulted due to link initialization failure.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that an encryption-configured port failed because of a link initialization failure.

Recommended Action

Disable and enable the port, and if the problem persists, replace the blade.

C5-1044**Message**

Trunk performance impact on port (<port number>) due to high deskew value. [TRUNK_PERF:<perf> percent, Deskew:<deskew>]

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates a high deskew value on the port.

Recommended Action

Check for physical cable length differences among physical ports of the trunk. If there are cable length differences, fix them with the same cable length link. Otherwise replace the cable if the problem persists.

C5-1045**Message**

Single parity error detected in ftb statistics memory, slot <slot> index <index>

Message Type

LOG

Message Severity

INFO

Probable Cause

A parity error was detected in FTB statistics memory; a Flow Vision flow monitor may show incorrect statistics.

Recommended Action

Reset the Flow Vision flow monitor flow that is showing abnormal statistics.

C5-1046**Message**

Multiple parity errors detected in ftb statistics memory, slot <slot> indexes <index> <index> <index> <index>

Message Type

LOG

Message Severity

INFO

Probable Cause

A parity error was detected in FTB statistics memory; a Flow Vision flow monitor may show incorrect statistics.

Recommended Action

Reset the Flow Vision flow monitor flow that is showing abnormal statistics.

C5-1048

Message

S<Slot number>,C<Chip Index>: Maximum possible buffers (<Maximum possible buffers>) exceeded; total desired:<Total Number of buffers desired>; port <Port with high desired count> has high desired count:<Desired buffer count on the one port> avail:0x<Available bufer count on the chip>

Message Type

LOG | FFDC

Message Severity

ERROR

Probable Cause

Probable Cause

More buffers have been requested/desired than exist on the ASIC. This will cause traffic disruption in the fabric.

Recommended Action

First, collect a supportsave and contact the switch vendor for analysis. If the number of requested buffers by the port is unexpectedly large, and if the port is a frontend port, toggle the identified port using portdisable, portenable, portcfgpersistentdisable, or portcfgpersistentenable. If that doesn't work, or if the port is a backend port, use slotpoweroff and slotpoweron on the identified blade. If the number of requested buffers makes sense and the current total ASIC buffers is very close to the ASIC maximum, contact the switch vendor to analyze switch data for possible ports to toggle and the next actions to take on the switch.

C5-1049

Message

S<Slot number>,P<User port index>(<Blade port number>): Port faulted at <String to identify location>. Requested <Maximum possible buffers> buffers; ASIC buffers: current=<Desired buffer count on the one port> max=<Total Number of buffers desired on ASIC>

Message Type

LOG | FFDC

Message Severity

ERROR

Probable Cause

More buffers have been requested/desired than exist on the ASIC. This will cause traffic disruption in the fabric.

Recommended Action

if the number of requested buffers by the port is unexpectedly large, and if the port is a frontend port, toggle the identified port using portdisable, portenable, portcfgpersistentdisable, or portcfgpersistentenable. If that doesn't work, or if the port is a backend port, use slotpoweroff and slotpoweron on the identified blade. If the number of requested buffers makes sense and the current total ASIC buffers is very close to the ASIC maximum, contact the switch vendor to analyze switch data for possible ports to toggle and the next actions to take on the switch.

C5-1050**Message**

S<Slot number>,C<Chip index>: No buffers allocated to <String to specify type of port> port. Requested <Maximum possible buffers> buffers; ASIC buffers: current=<Desired buffer count on the one port> max=<Total Number of buffers desired on ASIC>

Message Type

LOG | FFDC

Message Severity

ERROR

Probable Cause

More buffers have been requested/desired than exist on the ASIC. This will cause traffic disruption in the fabric.

Recommended Action

First, take a supportsave and contact the switch vendor for analysis. If the number of requested buffers by the port is unexpectedly large, or if the number of requested buffers makes sense and the current total ASIC buffers is very close to the ASIC maximum, contact the switch vendor to analyze switch data for possible ports to toggle and the next actions to take on the switch.

C5-1051**Message**

S<Slot number>,P<User port index>(<Blade port number>): (C:<chip index>) Port desired buffer mismatch. actual: <Actual desired buffer count on the port> expected: <Expected desired buffer count on the port> hw_scratch: <Hw scratch count on the port>

Message Type

LOG | FFDC

Message Severity

ERROR

Probable Cause

The number of buffers requested by a port does not match the number of buffers this port is supposed to request.

Recommended Action

First, collect a supportsave and contact the switch vendor. If the number of requested buffers by the port is unexpectedly large, and if the port is a frontend port, toggle the identified port using portdisable, portenable, portcfgpersistentdisable, or portcfgpersistentenable. If that doesn't work, or if the port is a backend port, use slotpoweroff and slotpoweron on the identified blade.

C5-1052**Message**

S<Slot number>,C<Chip index>: <String to specify type of port> port desired buffer mismatch. actual: <Actual desired buffer count on the port> expected: <Expected desired buffer count on the port>

Message Type

LOG | FFDC

Message Severity

ERROR

Probable Cause

The number of buffers requested by a port does not match the number of buffers this port is supposed to request.

Recommended Action

First, take a supportsave and contact the switch vendor for analysis. If the number of requested buffers by the port is unexpectedly large, contact the switch vendor to analyze switch data for the next actions to take on the switch.

C5-1053**Message**

S<slot number>,P<port number>(<blade port number>): 4G Speed is supported for F-Port only.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the E-Port is operating at 4G speed. The 4G speed is supported only on F_Ports.

Recommended Action**C5-1054****Message**

S<slot number>,P<port number>(<blade port number>): Media initialization fault; please reseal or replace media
rtryctr:<retries left>/<max retries > rate:<High(2)/Low rate(1)> failure:<failure code>.

Message Type

LOG | FFDC

Message Severity

ERROR

Probable Cause

A Media initialization fault occurs because the media is not seated properly or the SFP is faulty.Actions such as media plug-out/plug-in and switch power-cycle can cause this fault.

Recommended Action

Follow these steps: 1. Disable the port, and then enable it. 2. Reseat the media. 3. If reseating does not recover the module, replace the module.

C5-1055**Message**

Port in Slot <slot number>, Port <port number>(<blade port number>) getting faulted with reason <port fault reason>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the port has faulted because of errors.

Recommended Action

Disable and enable the port, and if the problem persists, replace the blade.

C5-1056**Message**

Chip in Slot <slot number>, Chip <chip index> getting faulted with reason <Fault reason>.

Message Type

LOG

Message Severity

CRITICAL

Probable Cause

Indicates that above-normal errors were observed in the hardware and the chip has faulted.

Recommended Action

When this error is observed persistently, power-cycle the specified blade using the `slotPowerOff` and `slotPowerOn` commands. If the problem persists, replace the blade.

C5-1057**Message**

S<slot number>,C<chip index>: HW ASIC Chip is in an inconsistent state = 0x<chip error>.

Message Type

LOG

Message Severity

CRITICAL

Probable Cause

Indicates that an internal error has been observed in the application-specific integrated circuit (ASIC) hardware that may degrade the data traffic.

Recommended Action

To recover a bladed system, execute the `slotPowerOff` and `slotPowerOn` commands on the blade. To recover a nonbladed system, execute the `fastBoot` command on the switch at the next customer maintenance window.

CAL Messages

Common Access Layer (CAL) error messages.

CAL-1001**Message**

Switch offline requested by remote domain <domain number>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the specified remote domain requested the local domain to be disabled.

Recommended Action

Check the error message log on the remote domain using the `errShow` command to find the reason.

CDR Messages

Driver error messages.

CDR-1001

Message

Port <port number> port fault. Change the SFP or check cable.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates a deteriorated small form-factor pluggable (SFP) transceiver, an incompatible SFP transceiver pair, a faulty cable between the peer ports, or that the port speed configuration does not match the capability of the SFP transceiver.

Recommended Action

Verify that compatible SFP transceivers are used on the peer ports, that the SFP transceivers have not deteriorated, and that the Fibre Channel cable is not faulty. Replace the SFP transceivers or the cable if necessary.

CDR-1002

Message

Port <port number> chip faulted due to internal error.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates an internal error. All the ports on the blade or switch will be disrupted.

Recommended Action

To recover a bladed system, execute the `slotPowerOff` and `slotPowerOn` commands on the blade. To recover a nonbladed system, execute the `fastBoot` command on the switch.

CDR-1003**Message**

S<slot number>,C<chip index>: HW ASIC Chip error type = 0x<chip error type>. If the problem persists, blade may need to be reset or replaced.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates an internal error in the application-specific integrated circuit (ASIC) hardware that may degrade the data traffic.

Recommended Action

Restart the system at the next customer maintenance window. If the problem persists, replace the blade.

CDR-1004**Message**

S<slot number>,C<chip index>: Invalid DMA ch pointer, chan:<Channel number>, good_addr:0x<Good address>
bad_addr:0x<Bad address>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates an internal error in the application-specific integrated circuit (ASIC) hardware that may degrade the data traffic.

Recommended Action

Restart the system at the next customer maintenance window. If the problem persists, replace the blade.

CDR-1005

Message

S<slot number>,P<port number>(<blade port number>): best effort QoS will be turned off at next port state change as it is not supported under this configuration.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that Quality of Service (QoS) will be turned off automatically at the next port state change because best effort QoS is no longer supported on 4Gb/s or 8Gb/s platform long-distance ports.

CDR-1006

Message

S<slot number>,P<port number>(<blade port number>): QoS overwrites portcfglongdistance vc_translation_link_init. ARB will be used on the link.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that Quality of Service (QoS) has overwritten the fill word IDLE used on the long-distance links. Arbitrated loop (ARB) will be used on the link.

CDR-1007

Message

S<slot number>,C<chip index>: Internal link errors have been reported, no hardware faults identified, continuing to monitor for errors: flt1:0x<fault1_cnt>, flt2:0x<fault2_cnt> thresh1:0x<threshold_used>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that some errors were found in the hardware that may or may not impact the data traffic.

CDR-1008**Message**

S<slot number>,C<chip index>: HW ASIC Chip warning Level 1 type = 0x<chip error type>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates an internal error in the application-specific integrated circuit (ASIC) hardware that may or may not degrade the data traffic.

Recommended Action

Restart the system at the next customer maintenance window.

CDR-1009**Message**

S<slot number>,C<chip index>: HW ASIC Chip warning Level 2 type = 0x<chip error type>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates an internal error in the application-specific integrated circuit (ASIC) hardware that may or may not degrade the data traffic.

Recommended Action

Restart the system at the next customer maintenance window.

CDR-1010

Message

S<slot number>,C<chip index>: Internal monitoring of faults has identified suspect hardware, blade may need to be reset or replaced: fault1:0x<fault1_cnt>, fault2:0x<fault2_cnt> thresh2:0x<threshold_used>.

Message Type

LOG

Message Severity

CRITICAL

Probable Cause

Indicates that above-normal errors were observed in the hardware that may or may not impact the data traffic.

Recommended Action

When this error is observed persistently, power-cycle the specified blade using the `slotPowerOff` and `slotPowerOn` commands. If the problem persists, replace the blade.

CDR-1011

Message

S<slot number>,P<port number>(<blade port number>): Link Timeout on internal port ftx=<frame transmitted> tov=<real timeout value> (><expected timeout value>) vc_no=<vc number> crd(s)lost=<Credit(s) lost> complete_loss:<complete credit loss>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that one or more credits have been lost on a back-end port and that there has been no traffic on that port for two seconds.

Recommended Action

Turn on back-end credit recovery to reset the link and recover the lost credits. If credit recovery has already been turned on, the link will be reset to recover the credits and no action is required.

CDR-1012

Message

S<slot number>,P<port number>(<blade port number>): Port Fault: Hard <Hard fault>(<Fault reason>) fault1=<Fault1 count> fault2=<Fault2 count> (0x<LIP and LLI fault count> 0x<RX_FIFO and HSS fault count> 0x<BWAIT fault count>).

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the specified port has failed. Port initialization will be retried.

Recommended Action

Replace the SFP transceiver and the cable and then re-enable the port.

CDR-1014

Message

Link Reset on Internal Port S<slot number>,P<port number>(<blade port number>) vc_no=<vc number> crd(s)lost=<Credit(s) lost>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that one or more credits were lost and that the link was reset.

Recommended Action

When this error is observed persistently, power-cycle the specified blade using the `slotPowerOff` and `slotPowerOn` commands. If the problem persists, replace the blade.

CDR-1015

Message

Port re-initialized due to Link Reset failure on internal Port S<slot number>,P<port number>(<blade port number>).

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the specified port was re-initialized due to a link reset failure.

Recommended Action

When this error is observed persistently, power-cycle the specified blade using the `slotPowerOff` and `slotPowerOn` commands. If the problem persists, replace the blade.

CDR-1016**Message**

Port is faulted due to port re-initialization failure on internal Port S<slot number>,P<port number>(<blade port number>) with reason <port fault reason>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the specified port has faulted due to a port re-initialization failure.

Recommended Action

When this error is observed persistently, power-cycle the specified blade using the `slotPowerOff` and `slotPowerOn` commands. If the problem persists, replace the blade.

CDR-1017**Message**

Blade in Slot <slot number> faulted due to unavailable ports in internal Trunk.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the specified blade has faulted due to unavailable ports in the internal trunk.

Recommended Action

When this error is observed persistently, power-cycle the specified blade using the `slotPowerOff` and `slotPowerOn` commands. If the problem persists, replace the blade.

CDR-1018**Message**

Blade in Slot <slot number> faulted due to Link reset threshold value exceeded.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the specified blade has faulted because the link reset threshold was exceeded.

Recommended Action

When this error is observed persistently, power-cycle the specified blade using the `slotPowerOff` and `slotPowerOn` commands. If the problem persists, replace the blade.

CDR-1019**Message**

S<slot number>,C<chip index>: HW ASIC Chip TXQ FID parity error threshold reached type = 0x<chip error type>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that an internal error was observed in the application-specific integrated circuit (ASIC) hardware that may degrade the data traffic.

Recommended Action

Restart the system at the next customer maintenance window.

CDR-1022

Message

S<slot number>,P<port number>(<blade port number>): Link Timeout on External port, ftx=<frame transmitted> tov=<real timeout value> (><expected timeout value>) vc_no=<vc number> crd(s)lost=<Credit(s) lost>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that above-normal errors were observed in the hardware that may or may not impact the data traffic.

Recommended Action

When this error is observed persistently, power-cycle the specified blade using the `slotPowerOff` and `slotPowerOn` commands. If the problem persists, replace the blade.

CDR-1028

Message

Detected excessive Link resets on the port in a second. Slot <slot number>, Port <port number>(<blade port number>).

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the port received excessive link resets from the peer port within 1 second and that the threshold was exceeded.

Recommended Action

When this error is observed persistently, change the small form-factor pluggable (SFP) transceiver or the cable on the peer port to which this port is connected.

CFG Messages

CFG module error messages.

CFG-1001

Message

Cfg info = <Error message>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Error message

Recommended Action

CFG-1002

Message

Failure in cfg component

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that a syntax error occurred when trying to launch the cfg process

Recommended Action

Execute the `firmwareDownload` command to reinstall the firmware.

If the message persists, execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

CH Messages

Command history messages.

CH-1001

Message

CLI history shell CLI buffer is disabled.

Message Type

AUDIT

Message Class

CLI

Message Severity

INFO

Probable Cause

Indicates that the CLI history shell CLI buffer has been disabled.

CH-1002

Message

CLI history shell CLI buffer is enabled.

Message Type

AUDIT

Message Class

CLI

Message Severity

INFO

Probable Cause

Indicates that the CLI history shell CLI buffer has been enabled.

CHS Messages

Error messages reporting the problems in the management of blades in different slots of the chassis.

CHS-1002

Message

ki_gd_register_action failed with rc = <return val>.

Message Type

LOG | FFDC

Message Severity

ERROR

Probable Cause

Indicates an internal error.

Recommended Action

To recover a bladed system, execute the `slotPowerOff` and `slotPowerOn` commands on the blade. To recover a non-bladed system, execute the `fastBoot` command on the switch.

CHS-1003

Message

Slot ENABLED but Not Ready during recovery, disabling slot = <slot number> rval = <return value>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the slot state has been detected as inconsistent during failover or recovery.

Recommended Action

For a bladed switch, execute the `slotPowerOff` and `slotPowerOn` commands to power cycle the blade.

For a non-bladed switch, restart or power cycle the switch.

CHS-1004

Message

Blade attach failed during recovery, disabling slot = <slot number>, rval = <return value>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the specified blade has failed during failover or recovery.

Recommended Action

For a bladed switch, execute the `slotPowerOff` and `slotPowerOn` commands to power cycle the blade.

For a non-bladed switch, restart or power cycle the switch.

CHS-1005

Message

Diag attach failed during recovery, disabling slot = <slot number>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the diagnostic blade attach operation has failed during failover or recovery.

Recommended Action

For a bladed switch, execute the `slotPowerOff` and `slotPowerOn` commands to power cycle the blade.

For a non-bladed switch, restart or power cycle the switch.

CHS-1006

Message

Chassis has been enabled.

Message Type

AUDIT

Message Class

CLI

Message Severity

INFO

Probable Cause

Indicates that the chassis is being intentionally enabled.

CHS-1007

Message

Chassis has been disabled.

Message Type

AUDIT

Message Class

CLI

Message Severity

INFO

Probable Cause

Indicates that the chassis is being intentionally disabled.

CHS-1008

Message

Chassis beacon has been <printf>.

Message Type

AUDIT

Message Class

CLI

Message Severity

INFO

Probable Cause

Indicates that the chassis beaconing is being enabled/disabled.

CNM Messages

Cluster Node Manager (CNM) module error messages.

CNM-1001

Message

Failed to allocate memory: (<function name>).

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the specified function has failed to allocate memory.

Recommended Action

Check memory usage on the switch using the `memShow` command.

Restart or power-cycle the switch.

CNM-1002

Message

Failed to initialize <module> rc = <error>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the initialization of a module within the Cluster Node Manager (CNM) has failed.

Recommended Action

Download a new firmware version using the `firmwareDownload` command.

CNM-1003

Message

Crypto device cfg between local switch (<local domain id>) and peer (<peer domain id>) out of sync. New encryption session not allowed.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the encryption engine nodes in the cluster encryption group have different configurations.

Recommended Action

Synchronize the configuration in the cluster group using the `cryptocfg` command.

CNM-1004**Message**

iSCSI service is <status> on the switch.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the crypto service has been enabled or disabled on the switch.

CNM-1005**Message**

Posting event CNM_EVT_GRP_LEADER_ELECTED Name [<nodeName>], WWN [<WWN>].

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the cluster Encryption Group (EG) leader has been elected.

CNM-1006**Message**

Posting event CNM_EVT_NODE_JOIN nodeName [<nodeName>], WWN [<WWN>], ipaddress [<IP address>].

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the member node has joined.

CNM-1007**Message**

Posting event CNM_EVT_GRP_LEADER_FAILED Name [<nodeName>]

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the Encryption Group (EG) leader has failed.

CNM-1008**Message**

Posting event CNM_EVT_NODE_EJECT nodeName [<nodeName>], WWN [<WWN>].

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the specified node has been ejected from the Encryption Group (EG).

CNM-1009**Message**

Posting event CNM_EVT_STANDALONE_MODE.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the node is in standalone mode.

CNM-1010**Message**

Posting event CNM_EVT_CLUSTER_UDATA_UPDATE cid [<client id>], ulen [<udata len>].

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates the client data update.

CNM-1011**Message**

Posting event CNM_EVT_NODE_JOIN_TIMEOUT nodeName [<nodeName>], WWN [<wwn>], ipaddress [<ipAddr>].

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates the node join timeout.

Recommended Action

Take the peer node offline, and rejoin the node to the Encryption Group (EG).

CNM-1012**Message**

Posting event CNM_EVT_EG_DELETED.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the Encryption Group (EG) has been deleted.

CNM-1013**Message**

Posting event GL Node Split condition, isolating peer GL node <nodeName>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the Encryption Group (EG) has been split.

CNM-1014**Message**

Posting event Node Admission Control passed, admitting node [<nodeName>].

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the node admission control was successful.

CNM-1015**Message**

Posting event Potential Cluster Split condition.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates a Potential Cluster Split condition.

CNM-1016**Message**

Posting event Detected a EG degrade condition.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates an Encryption Group (EG) degrade condition.

CNM-1017**Message**

Got JOIN REQUEST from un-recognized GL node [<rxglname>], configured GL node is [<glname>].

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that a join request was received from an invalid group leader (GL) node.

CNM-1018**Message**

Got CNM_FSM_EVT_JOIN_REQ when already a member, My assigned name [<nodename>], dropping request.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the node is already a member of the Encryption Group (EG).

CNM-1019

Message

Join Rejected by GL node, fix certificate and later add member node from GL node, or reboot the member node.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates an invalid member node certificate.

Recommended Action

Install a valid certificate and add a member node to the group leader (GL) node, or reboot the member node.

CNM-1020

Message

Node Admission Control failed due to mismatch in certificates, rejecting node [<nodename>].

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that node admission control has failed.

CNM-1021

Message

Failed to sign the node authentication message, admission control might fail.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that node admission control has failed.

CNM-1022

Message

Operation not allowed on GL Node.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that an operation is not allowed on a group leader (GL) node.

CNM-1023

Message

Group Leader node eject is not allowed.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that an eject operation is not allowed on a group leader (GL) node.

CNM-1024

Message

Operation not required on GL node.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that an operation is not required on a group leader (GL) node.

CNM-1025

Message

Operation not allowed, as member is active with the Cluster. Eject member node and retry.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that an operation is not allowed on a member node.

Recommended Action

Eject the member node and retry the operation.

CNM-1026

Message

Recvd HBT Msg with version mismatch, Recvd Hdr version 0x<received hardware version> Exp Hdr version 0x<expected hardware version> Node <WWN>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that a version mismatch has occurred.

Recommended Action

Upgrade the firmware or delete the node from the Encryption Group (EG).

CNM-1027**Message**

Received HBT from non-Group Member Node [<WWN>].

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that an operation is not allowed on a nongroup member node.

CNM-1028**Message**

Certfile <certificate file name> already exists. No need to sync up.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the certificate file for the node already exists.

CNM-1029**Message**

Certfile <certificate file name> content does not match the cert sent by GL.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the contents of the node's certificate file are different from the certificate file sent by the group leader (GL) node.

CNM-1030**Message**

Certfile <certificate file name> read less number of bytes <nbytes>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the read operation of the certificate file returned fewer bytes than expected.

CNM-1031**Message**

Certfile <certificate file name> open failed with errno <error num>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that an attempt to open the certificate file has failed.

CNM-1032**Message**

Certfile <certificate file name> size <file size> does not match cert file size <length> sent by GL.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that there is a size mismatch between a node's certificate file and the certificate file received from the group leader (GL).

CNM-1033**Message**

Some of the defined nodes in the Encryption Group are not ONLINE. Encryption Group is in degraded state.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the cluster is in a degraded state.

CNM-1034**Message**

All the defined nodes in the Encryption Group are ONLINE. Cluster is in converged state.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the cluster is in a converged state.

CNM-1035**Message**

Cluster is in degraded state. Posting degrade event.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that an event is being posted to specify that the cluster is in a degraded state.

CNM-1036**Message**

All the active nodes of the cluster are in ONLINE state. Posting converged event.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that an event is being posted to specify that the cluster is in a converged state.

CNM-1037**Message**

Split-Brain Arbitration lost, minority GL Node, remote:local [<remote_count>:<local_gl_ncount>].

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that split-brain arbitration has been lost.

CNM-1038**Message**

Split-Brain Arbitration won, majority GL Node, remote:local [<remote_count>:<local_gl_ncount>].

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that split-brain arbitration has been won.

CNM-1039**Message**

Split-Brain Arbitration lost, Minority WWN/GL Node, remote_WWN:local_WWN <wbuf>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that split-brain arbitration has been lost.

CNM-1040**Message**

Split-Brain Arbitration won, Majority WWN/GL Node, remote_WWN:local_WWN <WWN>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that split-brain arbitration has been won.

CNM-1041**Message**

Updating persistent Cluster DB, please avoid powering off the switch.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the system is updating the persistent database.

CNM-1042**Message**

Completed updating persistent Cluster DB.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the persistent database update is complete.

CNM-1043**Message**

Received HBT from undefined node IpAddress [<ip>], WWN [<wwn>]. Possible configuration error.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the remote node's WWN may have changed.

CNM-1044**Message**

Cluster Create Failed as the Certificate files not found, Please do the initnode.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the initnode has not been invoked.

Recommended Action

Execute the `cryptocfg --initnode` command.

CNM-1045

Message

Member node [<wwn>] is having dual IP stack. Registering member node with dual IP in an EG with only IPv6 is not allowed.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the member node with the dual IP stack was registered with the IPv6 Encryption Group (EG).

CNM-1046

Message

Posting event CNM_EVT_NODE_LEAVE nodeName [<nodeName>], WWN [<wwn>].

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the node has decided to leave the Encryption Group (EG).

CNM-1047

Message

Network Interface to Remote Node [<ip>] is [<string>].

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the status of the network interface is up or down.

CNM-1048**Message**

Posting <string>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates the event that is posted.

CNM-1049**Message**

Failed to define node, Node Name [<string>].

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates the failure to define the node object.

CNM-1050**Message**

Node Admission Control failed due to mismatch in Access Gateway Daemon (AGD) mode settings, rejecting node [<nodename>].

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates a mode mismatch between the switches, such as an Access Gateway mode mismatch.

CNM-1051

Message

Join Rejected by GL Node due to Access Gateway Daemon mode mismatch, ensure mode settings are same across all nodes in EG.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates a mode mismatch between the switches, such as an Access Gateway mode mismatch.

CNM-1052

Message

Member node registered with another Encryption Group. To proceed eject the member node [<nodename>] from other EG.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the member node is registered with another Encryption Group (EG).

CNM-1053

Message

Node is already a registered member of another EG. First eject the current node [<nodename>] from the existing EG and then try.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the node is already a registered member of another Encryption Group (EG).

Recommended Action

Eject the specified node from the EG and retry the operation.

CNM-1054

Message

Encryption Group database state [<state>] with node IP [<node>], WWN [<wwn>].

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates the status of the cluster database.

CNM-1055

Message

Got CNM_FSM_EVT_JOIN_REQ when already a member from same GL node, rejoining EG with GL [<glname>].

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the node is rejoining the Encryption Group (EG).

CNM-1056**Message**

Posting event CNM_EVT_EE_INITIALIZING Slot [<slot>], WWN [<wwn>], IP [<ip>], flags [<flags>].

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the encryption engine has been added into the Encryption Group (EG).

CNM-1057**Message**

Posting event CNM_EVT_ONLINE Slot [<slot>], WWN [<wwn>], IP [<ip>], flags [<flags>].

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the encryption engine is online in the Encryption Group (EG).

CNM-1058**Message**

Posting event CNM_EVT_OFFLINE Slot [<slot>], WWN [<wwn>], IP [<ip>], flags [<flags>].

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the encryption engine has been removed from the Encryption Group (EG).

CNM-1059**Message**

Local Node CP certificate pair mismatch detected, re-initialize the node.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the certificate pair is mismatched.

CNM-1060**Message**

Local Node CP certificate pair match detected.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the certificate pair is matched.

CNM-1061**Message**

IP of the switch changed from [<old_ip_address>] to [<new_ip_address>].

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the switch IP address has changed.

CNM-1062**Message**

Copied certificate to [<ofname>] due to change in IP.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the certificate was copied to the file with a new IP name.

CNM-3001**Message**

Event: cryptocfg Status: success, Info: encryption group \"<encryption_group_name>\" created.

Message Type

AUDIT | LOG

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates that the specified encryption group was created.

CNM-3002**Message**

Event: cryptocfg Status: success, Info: encryption group deleted.

Message Type

AUDIT | LOG

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates that an encryption group was deleted.

CNM-3003**Message**

Event: cryptocfg Status: success, Info: Membernode \"<member_node_WWN>\" added to encryption group.

Message Type

AUDIT | LOG

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates that the specified member node was added to an encryption group.

CNM-3004**Message**

Event: cryptocfg Status: success, Info: Membernode \"<member_node_WWN>\" ejected from encryption group.

Message Type

AUDIT | LOG

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates that the specified member node was ejected from an encryption group.

CNM-3005

Message

Event: cryptocfg Status: success, Info: Membernode \"<member_node_WWN>\" left encryption group.

Message Type

AUDIT | LOG

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates that the specified member node left an encryption group.

CNM-3006

Message

Event: cryptocfg Status: success, Info: Heartbeat miss count set to <heartbeat_misses>.

Message Type

AUDIT | LOG

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates that the heartbeat miss value was set.

CNM-3007

Message

Event: cryptocfg Status: success, Info: Heartbeat timeout set to <heartbeat_timeout>.

Message Type

AUDIT | LOG

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates that the heartbeat timeout value was set.

CNM-3008**Message**

Event: cryptocfg Status: success, Info: Routing mode of EE in slot <slot> set to <routingmode>.

Message Type

AUDIT | LOG

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates that the encryption engine routing mode was set.

CNM-3009**Message**

Event: cryptocfg Status: success, Info: <nodeType> <nodeWWN> registered.

Message Type

AUDIT | LOG

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates that the specified member node was registered.

CNM-3010

Message

Event: cryptocfg Status: success, Info: Membernode <membernodeWWN> unregistered.

Message Type

AUDIT | LOG

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates that the specified member node was unregistered.

CNM-3011

Message

Event: cryptocfg Status: success, Info: Encryption group synchronized.

Message Type

AUDIT | LOG

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates that an encryption group was synchronized.

CNM-3012

Message

Deleting an EG with LUNs setup for encryption can lead to LUNs being disabled if Encryption Group name is not preserved (<egName>).

Message Type

AUDIT | LOG

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates that the Encryption Group (EG) was deleted. Re-create the EG with the same name if LUNs are set up for encryption.

Recommended Action

Preserve the EG name when the EG is re-created if LUNs are set up for encryption.

CNMC Messages

Controller Area Network Management Interface Controller (CANMIC) module error messages.

CNMC-1001

Message

Switch reset to default configuration due to movement detection.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that a movement of the switch has occurred.

CNMC-1002

Message

Switch reset to default configuration upon receiving a request from Enclosure Manager.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the switch has received a reset to default configuration request from the Enclosure Manager.

CNMC-1003**Message**

Switch reset to default configuration failed (<Error code.>).

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the reset to default configuration request from the Enclosure Manager failed.

CONF Messages

Status messages for `configUpload` and `configDownload` operations.

CONF-1000**Message**

`configDownload` completed successfully <Info about the parameters and AD>.

Message Type

LOG | AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the `configDownload` operation was initiated and completed successfully. The *information about the parameters and AD* variable is the description of the classes of configuration parameters that were downloaded. If Admin Domain (AD) is enabled, the AD number is specified in the description.

CONF-1001

Message

configUpload completed successfully <Info about the parameters and AD>.

Message Type

LOG | AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the `configUpload` operation was initiated and completed successfully. The *information about the parameters and AD* variable is the description of the classes of configuration parameters that were uploaded. If Admin Domain (AD) is enabled, the AD number is specified in the description.

CONF-1020

Message

configDownload not permitted <AD Number if AD is configured on the system>.

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that a `configDownload` operation was not permitted. There are many possible causes.

Recommended Action

Execute the `errShow` command to view the error log. Correct the error and execute the `configDownload` command again.

CONF-1021

Message

configUpload not permitted <AD Number if AD is configured on the system>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that a `configUpload` operation was not permitted. There are many possible causes.

Recommended Action

Execute the `errShow` command to view the error log. Correct the error and execute the `configUpload` command again.

CONF-1022

Message

Downloading configuration without disabling the switch was unsuccessful.

Message Type

AUDIT

Message Class

CFG

Message Severity

WARNING

Probable Cause

Indicates that an attempt to download the configuration without disabling the switch was unsuccessful because there are one or more parameters that require the switch to be disabled.

Recommended Action

Disable the switch using the `switchDisable` command and download the configuration.

CONF-1023

Message

configDownload failed <Message>.

Message Type

LOG | AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that a `configDownload` operation failed.

Recommended Action

Execute the `errShow` command to view the error log. Correct the error and execute the `configDownload` command again.

CONF-1024

Message

`configUpload` failed <Message>.

Message Type

LOG | AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that a `configUpload` operation failed.

Recommended Action

Execute the `errShow` command to view the error log. Correct the error and execute the `configUpload` command again.

CONF-1030

Message

Configuration database full, data not committed (key: <Key of failed configuration data>).

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the previous configuration commands have resulted in a database full condition. Configuration changes associated with the specified key were not applied.

Recommended Action

Use the `configure` command and various other commands to erase configuration parameters that are no longer required. As a last resort, execute the `configDefault` command and reconfigure the system.

CONF-1031**Message**

`configDefault` completed successfully <Message>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the `configDefault` command was initiated and completed successfully.

CONF-1032**Message**

`configRemove` completed successfully <Message>.

Message Type

LOG | AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the `configRemove` command was initiated and completed successfully.

CONF-1033

Message

Factoryreset operation is completed successfully.

Message Type

LOG | AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the `factoryreset` was initiated and completed successfully.

CONF-1040

Message

configDefault Failed. <Message>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that an error occurred while executing the `configDefault` command.

Recommended Action

Execute the `errShow` command to view the error log. Correct the error and execute the `configDefault` command again.

CONF-1041

Message

configRemove Failed. <Message>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that an error occurred while issuing the `configRemove` command.

Recommended Action

Execute the `errShow` command to view the error log. Correct the error and execute the `configRemove` command again.

CONF-1042

Message

Fabric Configuration Parameter <Parameter> changed to <Value>.

Message Type

LOG | AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the fabric configuration parameter value has been changed.

CONF-1043

Message

Fabric Configuration Parameter <Parameter> changed to <Value>.

Message Type

LOG | AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the fabric configuration parameter value has been changed.

CONF-1044

Message

Fabric Configuration Parameter <Parameter> changed from <Old_Location> to <New_Location>.

Message Type

LOG | AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the fabric configuration parameter value has been changed by a user.

CONF-1045

Message

Dynamic port name is <Value>.

Message Type

LOG | AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the dynamic port name has been enabled or disabled.

CONF-1046

Message

<Parameter> changed to <Value>

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the configure command configuration value has been changed.

CONF-1047**Message**

Aptpolicy is updated to <Value>.

Message Type

LOG | AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the Advanced Performance Tuning policy has been updated successfully.

CONF-1048**Message**

Dynamic port name format is set to <Value>.

Message Type

LOG | AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the dynamic port name format has been changed.

CONF-1049

Message

Chassis CSCTL mode changed to <printf>.

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

The user changed the CSCTL mode via the CLI.

CONF-1050

Message

Chassis configuration - Secure config upload/download <Parameter>.

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

CLI : configurechassis

CONF-1051

Message

Chassis configure - Uploaded file suffix <Parameter>.

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

CLI : configurechassis

CONF-1052**Message**

Chassis configure - Auto firmware sync <Parameter>.

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

CLI: configurechassis

CONF-1053**Message**

Eth Rate Limiting feature is turned <Value>.

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

CLI: Configure

CONF-1054

Message

VF has been enabled.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the Virtual Fabric has been enabled.

CONF-1055

Message

VF has been disabled.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the Virtual Fabric has been disabled.

DIAG Messages

Diagnostic error messages.

DIAG-1000

Message

<Part1 of diag err string>

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates diagnostic errors on the console.

ECC Messages

Error Checking and Correction (ECC) error messages.

ECC-1000

Message

ECC Error <Multiple or single occurrence of errors of a given type detected> occurrence of <Automatic calibration error detected><Multiple bit error detected><Single bit error detected><Memory select error detected>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the processor memory controller has detected one of the several types of double data rate (DDR) memory errors. Single bit errors are corrected, but other errors indicate either software errors or problems with the target system DRAM. Single bit errors can be expected to occur infrequently and can be caused by uncontrollable external events like cosmic rays, but frequent single bit errors can be indications of a degrading DRAM device.

Recommended Action

Frequent single bit errors and all other error types should be reported to technical support for further action.

ECC-1001

Message

ECC Error <Multiple or single occurrence of multiple bit ECC error detected><Multiple or single occurrence of single bit ECC error detected><Multiple of single occurrence of access outside the defined physical memory space detected> detected.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the processor memory controller has detected one of the several types of double data rate (DDR) memory errors. Single bit errors are corrected, but other errors indicate either software errors or problems with the target system

DRAM. Single bit errors can be expected to occur infrequently and can be caused by uncontrollable external events like cosmic rays, but frequent single bit errors can be indications of a degrading DRAM device.

Recommended Action

Frequent single bit errors and all other error types should be reported to technical support for further action.

EM Messages

Environmental Monitor (EM) error messages.

EM-1001

Message

<FRU ID> is shutting down due to environmental limits.

Message Type

FFDC | LOG

Message Severity

CRITICAL

Probable Cause

Indicates that the specified field-replaceable unit (FRU) is shutting down because it exceeded an environmental policy threshold or limit. This event is typically a result of the FRU exceeding allowable operational thermal ranges or as a result of component failures.

Recommended Action

Verify that the location temperature is within the operational range of the switch. Refer to the *hardware reference manual* for the environmental temperature range of your switch.

Execute the `fanShow` command to verify that all fans are running at normal speeds. If any fans are missing or not performing at a high enough speed, they should be replaced.

Refer to the *hardware reference manual* for more information about the operational environmental limits and related policies.

EM-1002

Message

System fan(s) status <fan FRU>.

Message Type

LOG | FFDC

Message Severity

INFO

Probable Cause

Indicates that a nonbladed system has overheated and may shut down. All fan speeds are dumped to the console.

Recommended Action

Verify that the location temperature is within the operational range of the switch. Refer to the *hardware reference manual* for the environmental temperature range of your switch.

Execute the `fanShow` command to verify that all fans are running at normal speeds. If any fans are missing or are not performing at a high enough speed, they should be replaced.

EM-1003**Message**

<FRU ID> has an unknown hardware identifier: FRU faulted.

Message Type

FFDC | LOG

Message Severity

CRITICAL

Probable Cause

Indicates that a field-replaceable unit (FRU) header could not be read or is not valid. The FRU is faulted.

Recommended Action

Execute the `diagPost` command to ensure that the power-on self-test (POST) is enabled; then power-cycle the blade by using the `slotPowerOff` and `slotPowerOn` commands or have the blade's ejector switch cycled to run the POST and verify that the blade does not have any hardware problems.

EM-1004**Message**

<FRU ID> failed to power on.

Message Type

FFDC | LOG

Message Severity

CRITICAL

Probable Cause

Indicates that the specified field-replaceable unit (FRU) failed to power on and is not being used.

The *FRU ID* value is composed of an FRU type string and an optional number to identify the unit, slot, or port.

The Brocade 300 Switch has four fans and one power supply, but these parts cannot be replaced: the entire switch is an FRU.

Recommended Action

Reseat the FRU. If the problem persists, replace the FRU.

EM-1005**Message**

<FRU Id> has faulted. Sensor(s) above maximum limits.

Message Type

FFDC | LOG

Message Severity

CRITICAL

Probable Cause

Indicates that a blade in the specified slot or the switch (for nonbladed switches) is shut down for environmental reasons; its temperature or voltage is out of range.

Recommended Action

Check the environment and ensure the room temperature is within the operational range of the switch. Execute the `fanShow` command to verify that the fans are operating properly. Ensure that there are no blockages of the airflow around the chassis. If the temperature problem is isolated to the blade itself, replace the blade.

Voltage problems on a blade are likely a hardware problem on the blade itself; replace the blade.

EM-1006**Message**

<FRU Id> has faulted. Sensor(s) below minimum limits.

Message Type

FFDC | LOG

Message Severity

CRITICAL

Probable Cause

Indicates that the voltage on the switch is below minimum limits. The switch or specified blade is being shut down for environmental reasons; the voltage is too low.

Recommended Action

If this problem occurs on a blade, it usually indicates a hardware problem on the blade; replace the blade.

If this problem occurs on a switch, it usually indicates a hardware problem on the main board; replace the switch.

EM-1008**Message**

Unit in <Slot number or Switch> with ID <FRU Id> is faulted, it is incompatible with the <type of incompatibility> configuration, check FOS firmware version as a possible cause.

Message Type

FFDC | LOG

Message Severity

CRITICAL

Probable Cause

Indicates that a blade inserted in the specified slot or switch (for nonbladed switches) is not compatible with the platform configuration (includes the firmware version) or the switch configuration. The blade is faulted.

Recommended Action

If the blade is incompatible, upgrade the firmware or replace the blade and ensure that the replacement blade is compatible with your control processor (CP) type and firmware.

If the incompatibility is with the logical switch configuration, change the configuration by using the `lscfg` command to be consistent with the blade type, or remove the blade.

EM-1009**Message**

<FRU Id> powered down unexpectedly.

Message Type

FFDC | LOG

Message Severity

CRITICAL

Probable Cause

Indicates that the environmental monitor (EM) received an unexpected power-down notification from the specified field-replaceable unit (FRU). This may indicate a hardware malfunction in the FRU.

Recommended Action

Reseat the FRU. If the problem persists, replace the FRU.

EM-1010**Message**

Received unexpected power down for <FRU Id> But <FRU Id> still has power.

Message Type

FFDC | LOG

Message Severity

CRITICAL

Probable Cause

Indicates that the environmental monitor (EM) received an unexpected power-down notification from the specified field-replaceable unit (FRU). However, the specified FRU still appears to be powered up after four seconds.

Recommended Action

Reseat the blade. If the problem persists, replace the blade.

EM-1011**Message**

Received unexpected power down for <FRU Id>, but cannot determine if it has power.

Message Type

FFDC | LOG

Message Severity

CRITICAL

Probable Cause

Indicates that the environmental monitor (EM) received an unexpected power-down notification from the specified field-replaceable unit (FRU). However, after four seconds, it cannot be determined if it has powered down or not.

Recommended Action

Reseat the blade. If the problem persists, replace the blade.

EM-1012

Message

<FRU Id> failed <state> state transition, unit faulted.

Message Type

FFDC | LOG

Message Severity

CRITICAL

Probable Cause

Indicates that a switch blade or nonbladed switch failed to transition from one state to another. It is faulted. The specific failed target state is displayed in the message. There are serious internal Fabric OS configuration or hardware problems on the switch.

Recommended Action

Reseat the specified field-replaceable unit (FRU).

If the problem persists, restart or power cycle the switch.

Execute the `diagPost` command to make sure that power-on self-test (POST) is enabled; then power-cycle the blade by using the `slotPowerOff` and `slotPowerOn` commands or have the blade's ejector switch cycled to run POST and verify that the blade does not have any hardware problems.

If the problem still persists, replace the FRU.

EM-1013

Message

Failed to update FRU information for <FRU Id>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the environmental monitor (EM) was unable to update the time alive or original equipment manufacturer (OEM) data in the memory of a field-replaceable unit (FRU).

Recommended Action

If you executed the `fruInfoSet` command, execute the command again; otherwise, the update is automatically attempted again. If it continues to fail, reseat the FRU.

If the problem persists, replace the FRU.

EM-1014

Message

Unable to read sensor on <FRU Id> (<Return code>).

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the environmental monitor (EM) was unable to access the sensors on the specified field-replaceable unit (FRU).

Recommended Action

Reseat the FRU. If the problem persists, replace the FRU.

EM-1015

Message

Warm recovery failed (<Return code>).

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that a problem was discovered when performing consistency checks during a warm boot.

Recommended Action

Monitor the switch. If the problem persists, restart or power-cycle the switch.

EM-1016

Message

Cold recovery failed (<Return code>).

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that a problem was discovered when performing consistency checks during a cold boot.

Recommended Action

Monitor the switch.

If the problem persists, execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

EM-1017**Message**

Uncommitted WWN change detected. Cold reboot required.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that a user did not commit a changed World Wide Name (WWN) value before performing a system restart, power cycle, or firmware download operation.

Recommended Action

Change and commit the new WWN value.

EM-1018**Message**

CP blade in slot <slot number> failed to retrieve current chassis type (<return code>/<error code>/0x<unit number>).

Message Type

FFDC | LOG

Message Severity

CRITICAL

Probable Cause

Indicates that there was a failure to read the chassis type from the system.

Recommended Action

Verify that the control processor (CP) blade is operational and is properly seated in its slot.

EM-1019**Message**

Current chassis configuration option (<Chassis config option currently in effect>) is not compatible with standby firmware version (Pre 4.4), cannot allow HA Sync.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the current chassis configuration option is not supported by the firmware on the standby control processor (CP). This is true even if the standby CP comes up and is operational. High availability (HA) synchronization of the CPs will not be allowed.

Recommended Action

Change the chassis configuration option to 1 using the `chassisConfig` command, or upgrade the firmware on the standby CP to the version running on the active CP.

EM-1020**Message**

Unit in <Slot number> with ID <FRU Id> is faulted, it's an FCoE blade and the Ethernet switch service is not enabled. Please run `<fosconfig --enable ethsw>`.

Message Type

FFDC | LOG

Message Severity

ERROR

Probable Cause

Indicates that a blade inserted in the specified slot requires the Ethernet switch service, which is not enabled. The blade is faulted.

Recommended Action

Execute the `fosconfig --enable ethsw` command to enable the Ethernet switch service. Note that this is a disruptive command, which requires the system to be restarted. Otherwise, remove the blade.

EM-1028**Message**

HIL Error: <function> failed to access history log for FRU: <FRU Id> (rc=<return code>).

Message Type

FFDC | LOG

Message Severity

WARNING

Probable Cause

Indicates a problem accessing the data on the World Wide Name (WWN) card field-replaceable unit (FRU) or on the WWN card storage area on the main logic board.

The problems were encountered when the software attempted to write to the history log storage to record an event for the specified FRU. The return code is for internal use only. This can indicate a significant hardware problem.

The *FRU ID* value is composed of an FRU type string and an optional number to identify the unit, slot, or port.

Recommended Action

If the problem persists, restart or power-cycle the switch.

If the problem still persists, replace the WWN card, or the switch (for nonbladed switches).

EM-1029**Message**

<FRU Id>, a problem occurred accessing a device on the I2C bus (<error code>). Operational status (<state of the FRU when the error occurred>) not changed, access is being retried.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the Inter-Integrated Circuit (I2C) bus had problems and a timeout occurred.

Recommended Action

This is often a transient error.

Watch for the EM-1048 message, which indicates that the problem has been resolved.

If the problem persists, check for loose or dirty connections. Remove all dust and debris before reseating the field-replaceable unit (FRU). If it continues to fail, replace the FRU.

EM-1031**Message**

<FRU Id> ejector not closed.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the environmental monitor (EM) has found a switch blade that is inserted, but at least one ejector switch is not latched. The blade in the specified slot is treated as not inserted.

Recommended Action

Close the ejector switch (raise the slider in most blades or completely screw in the upper thumbscrew) if the field-replaceable unit (FRU) is intended for use. Refer to the appropriate *hardware reference manual* for instructions on inserting the switch blades.

EM-1033**Message**

CP in <FRU Id> set to faulty because CP ERROR asserted.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the standby control processor (CP) has been detected as faulty. The high availability (HA) feature will not be available. This message occurs every time the other CP restarts, even as part of a clean warm failover. In most situations, this message is followed by the EM-1047 message, and no action is required for the standby CP; however, find the reason for the failover.

Recommended Action

If the standby CP was restarted, wait for the error to clear (execute the `slotShow` command to determine if it has cleared). Watch for the EM-1047 message to verify that this error has cleared.

If the standby CP continues to be faulty or if it was not intentionally restarted, check the error logs on the other CP (using the `errDump` command) to determine the cause of the error state.

Reseat the field-replaceable unit (FRU). If the problem persists, replace the FRU.

EM-1034**Message**

<FRU Id> set to faulty, rc=<return code>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the specified field-replaceable unit (FRU) has been marked as faulty for the specified reason.

Recommended Action

Reseat the FRU.

Execute the `diagPost` command to ensure that power-on self-test (POST) is enabled; then power-cycle the blade by using the `slotPowerOff` and `slotPowerOn` commands or have the blade's ejector switch cycled to run the POST and verify that the blade does not have any hardware problems.

If the problem persists, replace the FRU.

EM-1035**Message**

2 circuit paired Power Supplies are faulty, please check the <Switch side> AC main switch/circuit to see if it has power.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that both power supplies associated with one of the two main circuits are present but faulty, that the circuit's switch may have been turned off, or that the AC power source has been interrupted for that circuit.

The *switch side* value designates the circuit switch facing the cable side of the chassis, and is one of the following values:

- left - Controls the odd-numbered power supply units.
- right - Controls the even-numbered power supply units.

Recommended Action

Verify that the identified AC circuit switch is turned on, that the power cord is properly attached and undamaged, and that the power source is operating properly.

EM-1036

Message

<FRU Id> is not accessible.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the specified field-replaceable unit (FRU) is not present on the switch.

If the FRU is a World Wide Name (WWN) card, the default WWN and IP addresses are used for the switch.

Recommended Action

Reseat the FRU.

If the problem persists, restart or power-cycle the switch.

Execute the `diagPost` command to ensure that power-on self-test (POST) is enabled; then power-cycle the blade by using the `slotPowerOff` and `slotPowerOn` commands or have the blade's ejector switch cycled to run the POST and verify that the blade does not have any hardware problems.

If the problem still persists, replace the FRU.

EM-1037

Message

<FRU Id> is Ok.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the specified power supply is OK and no longer marked faulty; probably because its AC power supply has been turned on.

EM-1042**Message**

Important FRU header data for <FRU Id> is not valid.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the specified field-replaceable unit (FRU) has an incorrect number of sensors in its FRU header-derived information. This could mean that the FRU header was corrupted or read incorrectly, or corrupted in the object database, which contains information about all FRUs.

Recommended Action

Reseat the FRU. If the problem persists, replace the FRU.

EM-1043**Message**

Can't power <FRU Id> <state (on or off)>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the specified field-replaceable unit (FRU) cannot be powered on or off.

Recommended Action

The specified FRU is not responding to the commands and should be replaced.

EM-1044

Message

Can't power on <FRU Id>, its logical switch is shut down.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the specified field-replaceable unit (FRU) cannot be powered on because the associated logical switch is shut down.

Recommended Action

Execute the `switchStart` command on the associated logical switch.

EM-1045

Message

<FRU Id> is being powered <new state>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that an automatic power adjustment is being made because of the (predicted) failure of a power supply or the insertion or removal of a port blade. The *new state* value can be one of the following values:

- On - A port blade is being powered on because the power is available (a power supply was inserted or a port blade was removed or powered down).
- Off - A port blade has been powered down because of the (predicted) failure of the power supply.
- Down - A newly inserted port blade was not powered on because there was not enough power available.

Recommended Action

For a fully populated chassis, you must always operate the system with at least two power supplies for redundancy.

EM-1046

Message

Error status received for blade ID <id value> for the blade in slot <slot number>, <blade incompatibility type: platform, backplane, or switch configuration>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the specified blade is incompatible.

Recommended Action

If the listed blade ID is incorrect, the field-replaceable unit (FRU) header for the blade is corrupted and the blade must be replaced.

If the error is due to the platform, the listed blade ID is not supported for that platform (CP) type. Remove the blade from the chassis.

If the error is due to the backplane, the CP type (CP256) is not supported on that chassis (backplane revision D2). Remove the blade from the chassis.

If the error is due to the switch configuration, the logical switch configuration of the blade is incorrect. Execute the `lscfg` command to correct the switch or port configuration for the ports on the blade.

EM-1047

Message

CP in slot <slot number> not faulty, CP ERROR deasserted.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the control processor (CP) is no longer faulted. This message usually follows the EM-1033 message. The new standby CP is in the process of restarting and has turned off the CP_ERR signal.

EM-1048

Message

<FRU Id> I2C access recovered: state <current state>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the Inter-Integrated Circuit (I2C) bus problems have been resolved and I2C access to the field-replaceable unit (FRU) has become available again.

Recommended Action

No action is required. The EM-1048 message is displayed when the EM-1029 error is resolved.

EM-1049

Message

FRU <FRU Id> insertion detected.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that a field-replaceable unit (FRU) of the type and location specified by the *FRU ID* value was detected as having been inserted into the chassis.

EM-1050

Message

FRU <FRU Id> removal detected.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that a field-replaceable unit (FRU) of the type and location specified by the *FRU ID* value was removed from the chassis.

Recommended Action

Verify that the FRU was intended to be removed. If not, replace the FRU as soon as possible.

EM-1051**Message**

<FRU Id>: Inconsistency detected, FRU reinitialized.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that an inconsistent state was found in the field-replaceable unit (FRU). This occurs if the state of the FRU was changing during a failover. The FRU is reinitialized, and the traffic may have been disrupted.

EM-1057**Message**

Blade:<Slot Id> is getting reset:<Fault reason>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the blade is being automatically reset because of known resettable transient errors such as an ASIC parity error.

Recommended Action

No action is required if the switch does not reach the reset threshold for the switch or blade. If the reset threshold is reached on the switch or blade, the switch or blade will be faulted and should be replaced.

EM-1058

Message

Switch gets reset:<Fault reason>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the switch is being automatically reset because of a known resettable transient problem such as an ASIC parity error.

Recommended Action

No action is required if the switch does not reach the reset threshold for the switch or blade. If the reset threshold is reached on the switch or blade, the switch or blade will be faulted and should be replaced.

EM-1059

Message

<Slot number or Switch> with ID <Blade Id> may not be supported on this platform, check FOS firmware version as a possible cause.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that a blade inserted in the specified slot or switch (for nonbladed switches) is incompatible with the switch configuration software. The blade will not be completely usable.

The blade may be supported only by a later (or earlier) version of the firmware.

Recommended Action

Change the control processor (CP) firmware or replace the blade. Ensure the replacement is compatible with your switch type and firmware.

EM-1060

Message

Stopping synchronization of the system due to blade incompatibility with software version on standby CP.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that a blade in the system is not supported by the firmware on the standby control processor (CP).

Recommended Action

Remove all blades of this type or upgrade the standby CP. After appropriate action is taken, restart the standby CP or execute the `haSyncStart` command to enable high availability (HA) state synchronization. Until this is done, the system will remain out of synchronization.

EM-1061

Message

Synchronization halted. Remove all blades of type <Blade Type Id> or upgrade your standby CP, then reboot or run `haSyncStart`.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the blade in the system is not supported by the firmware on the standby control processor (CP).

Recommended Action

Remove all blades of the specified type or upgrade the standby CP. After appropriate action is taken, restart the standby CP or execute the `haSyncStart` command to enable high availability (HA) state synchronization. Until this is done, the system will remain out of synchronization.

EM-1062

Message

Blade in slot <Slot Id> faulted as it exceeds the maximum support limit of <Limit> blades with Blade ID <Blade Type Id> in the chassis.

Message Type

LOG

Message Severity

CRITICAL

Probable Cause

Indicates that too many blades of a particular type are in the system.

Recommended Action

Remove the faulted blade.

EM-1063

Message

Blade in slot <Slot Id> faulted because it exceeds the maximum support limit of <Limit> blades with Blade IDs <Applicable blade Type IDs> in the chassis.

Message Type

LOG

Message Severity

CRITICAL

Probable Cause

Indicates that too many blades of a set of particular types are in the system.

Recommended Action

Remove the faulted blade.

EM-1064

Message

Blade:<Slot Id> is being powered off (based on user configuration) upon receiving a HW ASIC ERROR, reason:<Fault reason>.

Message Type

LOG

Message Severity

CRITICAL

Probable Cause

Indicates that the blade is being powered off because a hardware (HW) ASIC error was detected and that you have selected to power off the problem blade when such a condition occurred.

Recommended Action

Contact your switch service provider for assistance.

EM-1065**Message**

SAS Virtualization Services are not available due to incompatibility between the FOS and SAS versions<Slot number or blank for single board systems>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the version of the control processor firmware (CFOS) or blade processor firmware (BFOS) is not compatible with the Storage Application Services (SAS) or other application firmware versions.

Recommended Action

Upgrade the Fabric OS firmware or the SAS firmware by using the `firmwareDownload` command. Refer to the release notes for a compatible version of firmware.

EM-1066**Message**

SAS Virtualization Services are now available <Slot number or blank for single board systems>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the previously incompatible Fabric OS or Storage Application Services (SAS) firmware has been upgraded and is now compatible.

EM-1067**Message**

Stopping synchronization of the system due to <version> incompatibility with standby CP.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the software version on the standby control processor (CP) is incompatible with the software feature enabled on this Fabric OS firmware version.

Recommended Action

Upgrade the software on the standby CP or disable the software feature on this CP.

To disable the Ethernet switch service, execute the `fosconfig --disable ethsw` command.

To view the buffer optimization mode for the slots, execute the `bufopmod --showall` command, and then execute the `bufopmode --reset slot` command to disable the feature for those slots before downgrading.

To disable FC8-16 Serdes tuning mode, execute the `serdestunemode --reset` command.

EM-1068**Message**

High Availability Service Management subsystem failed to respond. A required component is not operating.

Message Type

FFDC | LOG

Message Severity

ERROR

Probable Cause

Indicates that the high availability (HA) subsystem has not returned a response within four minutes of the request from the environmental monitor (EM). It usually indicates that some component has not started properly or has terminated. The specific component that has failed may be indicated in other messages or debug data. There are serious internal Fabric OS configuration or hardware problems on the switch.

Recommended Action

Restart or power-cycle the switch.

If the problem persists, execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

EM-1069**Message**

Slot <FRU slot number> is being powered off.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the blade in the specified slot is being intentionally powered off.

EM-1070**Message**

Slot <FRU slot number> is being powered on.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the blade in the specified slot is being intentionally powered on.

EM-1071**Message**

Unit in <Slot number> with ID <FRU Id> is faulted, it is incompatible with the following blade id(s): <blade incompatibility list>.

Message Type

FFDC | LOG

Message Severity

CRITICAL

Probable Cause

Indicates that a blade inserted in the specified slot is incompatible with another blade in the system.

Recommended Action

Determine which blade is essential to your configuration and remove blades that are incompatible with it.

EM-1072**Message**

Chassis cannot become ready since no Core Blades are available.

Message Type

FFDC | LOG

Message Severity

CRITICAL

Probable Cause

Indicates that all core blades are missing, faulted, or powered off. There must be at least one core blade in the enabled state for the chassis to be considered ready.

Recommended Action

Insert and close the ejector switch on missing core blades. Reseat or replace core blades that are faulted or powered off.

EM-1073**Message**

Blade devices cannot be accessed. The blade in slot <FRU slot number> is being moved to ABSENT state.

Message Type

FFDC | LOG

Message Severity

CRITICAL

Probable Cause

Indicates that the devices on the blade were not accessible. The blade is being transitioned to the ABSENT state.

Recommended Action

Reseat or replace the affected blade.

EM-1074**Message**

The ASIC in <FRU ID> is overheating: Shutting down.

Message Type

FFDC | LOG

Message Severity

CRITICAL

Probable Cause

Indicates that the ASIC present in switch is overheating and is beyond the thermal operating range. This event is typically due to a faulty fan and can also be caused by the switch environment.

Recommended Action

Verify that the location temperature is within the operational range of the switch. Refer to the *hardware reference manual* for the environmental temperature range of your switch.

Execute the `fanShow` command to verify that all fans are running at normal speeds. If any fans are missing or not performing at a high enough speed, they should be replaced.

EM-1075**Message**

<FRU Id> poweron was attempted while it was being powered off. The slot will remain powered off.

Message Type

LOG

Message Severity

WARNING

Probable Cause

The previous slot poweroff is yet to be completed and hence cannot process poweron of the slot. So the slot remains to be powered off. Wait till the slot poweroff process is complete.

Recommended Action

Wait till the slot poweroff process is complete

EM-1076

Message

Slot <slot number> blade-ID mismatch. To recover, please execute 'slotcfg --default -reset <slot number>' then slotpoweroff/slotpoweron for slot <slot number>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that current blade-id has changed compared to old blade_id.

Recommended Action

Execute `slotcfg --default -reset slot_number#` command to recover the faulty blade.

EM-1100

Message

Unit in <Slot number or Switch> with ID <FRU Id> is faulted(<Fault>). <Current attempt number> of <Total number of attempts> total attempt(s) at auto-recovery is being made. Delay is <Delay time in seconds> seconds.

Message Type

FFDC | LOG

Message Severity

CRITICAL

Probable Cause

A fault that has been determined to be auto-recoverable has happened and recovery is being attempted.

Recommended Action

If auto-recovery does not happen gracefully within a reasonable time frame, follow the user guide to recover the blade.

EM-1101

Message

Unit in <Slot number or Switch> with ID <FRU Id> is faulted(<Fault>). <Current attempt number> attempt(s) at auto-recovery were made without success.

Message Type

LOG

Message Severity

CRITICAL

Probable Cause

A fault that has been determined to be auto-recoverable has happened, but recovery failed.

Recommended Action

Follow the user guide to recover the blade.

EM-1134

Message

<FRU Id> set to faulty, rc=<return code>.

Message Type

LOG | FFDC

Message Severity

ERROR

Probable Cause

Indicates that the specified field-replaceable unit (FRU) has been marked as faulty for the specified reason.

Recommended Action

Reseat the FRU.

Execute the `diagPost` command to ensure that power-on self-test (POST) is enabled; then power-cycle the blade by using the `slotPowerOff` and `slotPowerOn` commands or have the blade's ejector switch cycled to run the POST and verify that the blade does not have any hardware problems.

If the problem persists, replace the FRU.

EM-1220

Message

A problem (Error:<The return code is for internal use only>) has been detected on one or both WWN cards. Please run the `wwnrecover` tool to get more information and recovery options.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that a problem was found accessing one (or both) of the WWN cards or with the content of the data stored there. The content problem could be a corrupted data set or a mismatch between the two WWN cards.

Recommended Action

Execute the `wwnrecover` command to get details of the problems found and how to recover.

EM-1221**Message**

A WWN card insertion has been detected. WWN verification audit will be run to ensure no mismatches or other problems.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the second WWN card was enabled. Because the data may not match, the WWN verification audit will be run.

Recommended Action

If an EM-1220 follows, execute the `wwnrecover` command to get details of the problems found and how to recover. If an EM-1220 message does not follow, no action is required.

EM-1222**Message**

A WWN card access problem has been encountered. Please run the `wwnrecover` tool to get more information and recovery options.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that a problem was encountered while accessing one (or both) of the WWN cards or with the content of the data stored there.

Recommended Action

Execute the `wwnrecover` command to get details of the problems found and how to recover.

EM-1223**Message**

Slot <FRU slot number> has been powered on.

Message Type

AUDIT | LOG

Message Class

CLI

Message Severity

INFO

Probable Cause

Indicates that the blade in the specified slot is being intentionally powered on.

EM-1224**Message**

Slot <FRU slot number> has been powered off.

Message Type

AUDIT

Message Class

CLI

Message Severity

INFO

Probable Cause

Indicates that the blade in the specified slot is being intentionally powered off.

EM-1225

Message

Slot <FRU slot number> has been persistently powered off.

Message Type

AUDIT

Message Class

CLI

Message Severity

INFO

Probable Cause

Indicates that the blade in the specified slot is being intentionally powered off.

EM-1226

Message

Fan-<Fan unit number> has been <Enable config>.

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the specified fan unit is being enabled/disabled.

EM-1227

Message

Slot <FRU slot number> is being powered off as it was detected as faulty during previous INIT. Power-cycle the blade by using the command slotPowerOff and slotPowerOn.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the blade was detected as faulty in a previous reboot and that it is being intentionally powered off.

Recommended Action

Contact switch vendor or remove the faulty blade and run the slotpoweron command on the new blade.

EM-1228**Message**

The <FRU ID> sensor 0x<Sensor Code> value out of range: <Raw Sensor Value>/<Retry Count>: Excessive power consumption detected. Power down and replace this switch.

Message Type

LOG

Message Severity

CRITICAL

Probable Cause

Indicates that the switch is consuming excessive power.

Recommended Action

Power down and replace this switch.

EM-1229**Message**

Excessive power usage (<Total Power Consumed >W) detected (PS1=<PS 1 Power Consumed >W, PS2=<PS 2 Power Consumed >W). Monitor closely and power down/replace switch if this persists

Message Type

LOG

Message Severity

CRITICAL

Probable Cause

This Switch is reporting excessive power power consumption.

Recommended Action

This may be a spurious occurrence. Please monitor the switch closely. If this persists then power down and replace this switch.

EM-1230**Message**

Excessive power usage (<Total Power Consumed >W) detected (PS1=<PS 1 Power Consumed >W, PS2=<PS 2 Power Consumed >W). System is shutting down. Please replace switch if this persists

Message Type

LOG

Message Severity

CRITICAL

Probable Cause

This Switch is reporting excessive power power consumption.

Recommended Action

This may be a spurious occurrence. Switch is being shutdown. If this persists following powering back up, then replace this switch.

EM-1235**Message**

Platform and software release mismatch. Switch is being disabled. Please contact TAC support for Remedial action

Message Type

LOG

Message Severity

CRITICAL

Probable Cause

Periodic checking detected a mismatch in the FOS version and Switch Revision.

Recommended Action

The FOS version running on this does not match with the switch revision. The **firmwareDownload** command permits FOS to remedy this issue.

EM-1240

Message

Please note: This System will reach End of Support in <Number of days from today for system to reach End of Support > days.

Message Type

LOG

Message Severity

WARNING

Probable Cause

The system is within 90 days of reaching End of Support.

Recommended Action

This is a warning to alert the user of the impending End Of Support. User is advised to purchase and install extended End of Support to avoid restricted support functionality past End of Support.

EM-1241

Message

Please note: This System is now <Number of days this system has gone past End of Support > days past End of Support.

Message Type

LOG

Message Severity

WARNING

Probable Cause

The sytem is past End of Support.

Recommended Action

This is a warning to alert the user that the system is past End Of Support. User is advised to purchase and install extended End of Support to revert the restricted support functionality past End of Support.

EM-2003

Message

<Slot ID or Switch> has failed the POST tests. FRU is being faulted.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that a field-replaceable unit (FRU) has failed the power-on self-test (POST). Refer to the */tmp/post[1/2].slot#.log* file for more information on the faults. The ID will be Switch for nonbladed systems.

Recommended Action

On bladed systems, reseal the specified FRU.

On nonbladed switches, restart or power-cycle the switch.

If the problem persists, perform the following actions:

- Execute the `diagPost` command to ensure that POST is enabled; then power-cycle the blade by using the `slotPowerOff` and `slotPowerOn` commands or have the blade's ejector switch cycled to run the POST and verify that the blade does not have any hardware problems.
- On bladed systems, replace the specified FRU; otherwise, replace the switch.

EM-2004**Message**

<FRU Id>

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the user has set the blade to persistently disable mode.

ERCP Messages

Error Reporting Control Process (ERCP) error messages.

ERCP-1000**Message**

Multiple DDR ECC errors are detected and the system will reload automatically.

Message Type

FFDC | LOG

Message Severity

CRITICAL

Probable Cause

Indicates that error checking and correction (ECC) errors occurred due to multi-bit corruption.

Recommended Action

No action is required. The system will reload automatically to recover from the error.

ERCP-1001**Message**

Multiple CCF ECC errors are detected and the system will reload automatically.

Message Type

FFDC | LOG

Message Severity

CRITICAL

Probable Cause

Indicates that error checking and correction (ECC) errors occurred due to multi-bit corruption.

Recommended Action

No action is required. The system will reload automatically to recover from the error.

ERCP-1002**Message**

Multiple CPC ECC errors are detected and the system will reload automatically.

Message Type

FFDC | LOG

Message Severity

CRITICAL

Probable Cause

Indicates that error checking and correction (ECC) errors occurred due to multi-bit corruption.

Recommended Action

No action is required. The system will reload automatically to recover from the error.

ESM Messages

Extension Services Module (ESM) error messages.

ESM-1000

Message

ESMd <Module Name> initialization complete rc:<Return Code>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that ESMd module initialization phase has completed.

ESM-1001

Message

ESMd <Module Name> uninitialization complete rc:<Return Code>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that ESMd module uninitialization phase has completed.

ESM-1002

Message

ESMd initialization done for service <Service Name>:<Instance Number>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that ESMd service has initialized.

ESM-1003**Message**

ESMd uninitialization called for service <Service Name>:<Instance Number>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that ESMd service uninitialization phase has completed.

ESM-1004**Message**

ESMd failed to initialize <Module Name> rc:<Return Code>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the specified module has failed to initialize.

Recommended Action

If the message persists, execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

ESM-1005**Message**

Configuration (<Configuration>) replay failed - <Failure Reason>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates the specified configuration failed to be reapplied during config replay.

Recommended Action

Use the `portCfg`, `portShow`, and `portCfgShow` commands to correct the cause of the failure.

ESM-1010

Message

DP<DP ID> is OFFLINE.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the specified Data Processor (DP) has went offline.

Recommended Action

If the message persists, execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

ESM-1011

Message

DP<DP ID> is ONLINE.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that specified Data Processor (DP) has come online.

ESM-1012**Message**

DP<DP ID> Configuration replay has started.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that Data Processor (DP) configuration replay has started.

ESM-1013**Message**

DP<DP ID> Configuration replay has completed.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that Data Processor (DP) configuration replay has completed.

ESM-1100**Message**

<Warning message string.>

Message Type

LOG

Message Severity

WARNING

Probable Cause

Internal warning occurred as indicated by the warning message.

Recommended Action

If the message persists, execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

ESM-1101**Message**

<Error message string.>

Message Type

LOG

Message Severity

ERROR

Probable Cause

Internal error occurred as indicated by the error message.

Recommended Action

If the message persists, execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

ESM-1102**Message**

Unable to post DP<DP ID> ras evt:0x<Event ID> sig:<Event Signature> recv ver:0x<Event Version> due to CP/DP code mismatch.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates a different version in Remote Access Service (RAS) event message due to mismatch between the control processor (CP) and data processor (DP) versions.

Recommended Action

This is normal during extension Hot Code Load (HCL) and can be ignored if seen during the extension HCL process. If the message persists or is seen when not performing an extension HCL, execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

ESM-1103**Message**

Extension configurations for <Slot> have all been cleared.

Message Type

AUDIT | LOG

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates all extension configurations for slot(s) have been cleared.

ESM-1104**Message**

Extension configuration default for <Slot> completed.

Message Type

AUDIT | LOG

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates extension configurations for slot(s) have been reset to defaults.

ESM-1105

Message

<Type of stats> reset completed.

Message Type

AUDIT | LOG

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that reset has completed.

ESM-1106

Message

<Object Type> <Field Type> field has been changed: \"<Old String>\" -> \"<New String>\".

Message Type

AUDIT | LOG

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates the specified object type has had the specified field type changed from the old string value to the new string value. This is done to remove leading / trailing whitespace characters as well as any new-line and carriage return characters from the string to conform to a common string format. This will automatically update the configuration database as needed.

Recommended Action

No action is explicitly needed. If the New String value is not desirable, the configuration object can be modified and/or recreated with a more suitable string value using the appropriate command for the object type.

ESM-2000

Message

IP Interface <GE Port>.dp<DP ID> created <Address>/<Mask> vlan: <Vlan ID> mtu: <MTU> [<Originator>].

Message Type

AUDIT | LOG

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the specified IP interface has been added.

ESM-2001

Message

IP Interface <GE Port>.dp<DP ID> deleted <Address>/<Mask> [<Originator>].

Message Type

AUDIT | LOG

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the specified IP interface has been removed.

ESM-2002

Message

IP Interface <GE Port>.dp<DP ID> modified: <Address>/<Mask> vlan: <Vlan ID> mtu: <MTU> [<Originator>].

Message Type

AUDIT | LOG

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the specified IP interface has been modified.

ESM-2010

Message

IProute <GE Port>.dp<DP ID> create dest:<destination address>/<dest address prefix> gate:<gateway address> [<Originator>].

Message Type

AUDIT | LOG

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the specified IP route has been created.

ESM-2011

Message

IProute <GE Port>.dp<DP ID> deleted dest:<destination address>/<dest address prefix> gate:<gateway address> [<Originator>].

Message Type

AUDIT | LOG

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the specified IP route has been deleted.

ESM-2012**Message**

IProute <GE Port>.dp<DP ID> modified dest:<destination address>/<dest address prefix> gate:<gateway address> [<Originator>].

Message Type

AUDIT | LOG

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the specified IP route has been modified.

ESM-2100**Message**

VE tunnel <VE-Port> created [<Originator>].

Message Type

AUDIT | LOG

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the specified VE tunnel has been created.

ESM-2101**Message**

VE tunnel <VE-Port> deleted [<Originator>].

Message Type

AUDIT | LOG

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the specified VE tunnel has been deleted.

ESM-2102

Message

VE Tunnel <VE-Port> modified [<Originator>].

Message Type

AUDIT | LOG

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the specified VE Tunnel has been modified.

ESM-2103

Message

VE Tunnel <VE-Port> MODATTR (<Attribute change description>).

Message Type

AUDIT | LOG

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that an attribute has been changed for the specified VE Tunnel.

ESM-2104**Message**

VE Tunnel <VE-Port> is OFFLINE.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the operational status of the specified tunnel is offline.

Recommended Action

If the tunnel is not administratively down, a network error or disruption may have occurred.

ESM-2105**Message**

VE Tunnel <VE-Port> is DEGRADED.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the operational status of the specified tunnel has degraded.

Recommended Action

If the tunnel is not administratively down, a network error or disruption may have occurred.

ESM-2106**Message**

VE Tunnel <VE-Port> is ONLINE.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the specified VE Tunnel is online.

ESM-2200**Message**

VE Circuit <VE Port>.<Circuit ID> created [<Originator>].

Message Type

AUDIT | LOG

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the specified circuit has been created.

ESM-2201**Message**

VE Circuit <VE Port>.<Circuit ID> deleted [<Originator>].

Message Type

AUDIT | LOG

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the specified circuit has been deleted.

ESM-2202

Message

VE Circuit <VE Port>.<Circuit ID> modified [<Originator>].

Message Type

AUDIT | LOG

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the specified circuit has been modified.

ESM-2203

Message

VE Circuit <VE Port>.<Circuit ID> MODATTR (<Attribute change description>).

Message Type

AUDIT | LOG

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates an attribute changed for the specified VE circuit.

ESM-2300

Message

IPsec policy <Policy Name> added [<Originator>].

Message Type

AUDIT | LOG

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the specified Internet Protocol security (IPsec) policy has been added.

ESM-2301**Message**

IPsec policy <Policy Name> deleted [<Originator>].

Message Type

AUDIT | LOG

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the specified Internet Protocol security (IPsec) policy has been deleted.

ESM-2302**Message**

IPsec policy <Policy Name> modified [<Originator>].

Message Type

AUDIT | LOG

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the specified Internet Protocol security (IPsec) policy has been modified.

ESM-2303

Message

IPsec policy <Policy Name> MODATTR (<Attribute change description>).

Message Type

AUDIT | LOG

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates an attribute changed for the specified Internet Protocol security (IPsec) policy.

ESM-2310

Message

IKE Session Policy <IPSec Policy Name> dp<DP ID>.<IKE Session ID> created <Local IP Address> - <Remote IP Address>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the specified Internet Key Exchange (IKE) session has been created for the specified Internet Protocol security (IPsec) policy.

ESM-2311

Message

IKE Session Policy <IPSec Policy Name> dp<DP ID>.<IKE Session ID> deleted <Local IP Address> - <Remote IP Address>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the specified Internet Key Exchange (IKE) session has been deleted for the specified Internet Protocol security (IPsec) policy.

ESM-2312**Message**

Continuous health check failed on DP<DP ID>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that Federal Information Processing Standards (FIPS) continuous health check failure is detected by Internet Protocol Security (IPsec).

Recommended Action

Execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

ESM-2313**Message**

On-demand health check failed on DP<DP ID>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that Federal Information Processing Standards (FIPS) on-demand health check failure is detected by Internet Protocol Security (IPsec).

Recommended Action

Execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

ESM-2314**Message**

DP<DP ID> initiated data-plane zeroization.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that Federal Information Processing Standards (FIPS) failure is detected by Internet Protocol Security (IPsec).

Recommended Action

Execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

ESM-2315**Message**

POST failure detected on DP<DP ID>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that Federal Information Processing Standards (FIPS) Power-On Self-Test (POST) failure is detected by Internet Protocol Security (IPsec).

Recommended Action

Execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

ESM-2316

Message

Running self test on DP<DP ID>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that Federal Information Processing Standards (FIPS) self test is being run on a data processor (DP).

Recommended Action

Execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

ESM-2317

Message

Extension IPSEC verify operation for Session:<Session ID> Peer Certificate:<Certificate Name> failed.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the verify request from a data processor (DP) has failed on the control plane (CP).

Recommended Action

Execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

ESM-2318

Message

Extension IPSEC verify operation for Session:<Session ID> could not locate Peer Certificate:<Certificate Name>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the verify request could not be serviced because the certificate was missing.

Recommended Action

Execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

ESM-2319**Message**

Extension IPSEC sign operation for Session:<Session ID> Keypair:<Keypair Name> failed.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the sign request from a data processor (DP) has failed on the control plane (CP).

Recommended Action

Execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

ESM-2320**Message**

Extension IPSEC sign operation for Session:<Session ID> could not locate Keypair:<Keypair Name>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the sign request could not be serviced because the keypair was missing or incomplete.

Recommended Action

Execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

ESM-2321**Message**

Extension IPSEC verify operation for Session:<Session ID> failed since Peer Certificate:<Certificate Name> expired .

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the verify request could not be serviced because the certificate has expired.

Recommended Action

Execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

ESM-2322**Message**

Extension IPSEC sign operation for Session:<Session ID> failed since Keypair:<Keypair Name> certificate expired .

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the sign request could not be serviced because the keypair was missing or incomplete.

Recommended Action

Execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

ESM-2323

Message

IPSec Self test run failed on DP<DP ID>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that Federal Information Processing Standards (FIPS) self test is failed on a data processor (DP).

Recommended Action

Execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

ESM-2324

Message

Extension IPSEC verify operation for Session:<Session ID> found tampered Peer Certificate:<Certificate Name>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the verify request could not be serviced because the certificate was tampered.

Recommended Action

Execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

ESM-2325

Message

Extension IPSEC sign operation for Session:<Session ID> found tampered Keypair:<Keypair Name>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the sign request could not be serviced because the keypair was tampered.

Recommended Action

Execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

ESM-2326**Message**

Extension IPSEC verify operation for Session:<Session ID> found hash mismatch for Peer Certificate:<Certificate Name>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the verify request could not be serviced because the certificate did not match.

Recommended Action

Execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

ESM-2327**Message**

Extension IPSEC sign operation for Session:<Session ID> found hash mismatch for Keypair:<Keypair Name>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the sign request could not be serviced because the certificate did not match.

Recommended Action

Execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

ESM-2328**Message**

Extension IPsec Certificate:<Certificate Name> for Keypair:<Keypair Name> certificate has expired .

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the Internet Protocol security (IPsec) certificate has expired.

Recommended Action

Execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

ESM-2329**Message**

Restart authentication for IKE sessions on IPsec policy <IPsec Policy Name>.

Message Type

AUDIT | LOG

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that IPsec policy has restarted authentication on all faulty IKE sessions.

ESM-2400

Message

Blade configuration for slot <Slot> set to APP-Mode:<App-Mode> VE-Mode:<VE-Mode> GE-Mode:<GE-Mode> [<Originator>].

Message Type

AUDIT | LOG

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the blade configuration has been set to the specified App/VE/GE modes.

ESM-2700

Message

TCL <TCL Name> created [<Originator>].

Message Type

AUDIT | LOG

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that a Traffic Control List (TCL) has been created.

ESM-2701

Message

TCL <TCL Name> Modified [<Originator>].

Message Type

AUDIT | LOG

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that a Traffic Control List (TCL) has been modified.

ESM-2702**Message**

TCL <TCL Name> deleted [<Originator>].

Message Type

AUDIT | LOG

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that a Traffic Control List (TCL) has been deleted.

ESM-2703**Message**

TCL <TCL Name> admin status changed [<TCL Admin status>].

Message Type

AUDIT | LOG

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that a Traffic Control List (TCL) Internal admin status has changed.

ESM-2801

Message

Port <Port Name> speed set to <Port Speed>, auto negotiation <Autonegotiation state>, FEC clause <FEC Clause> [<App>].

Message Type

AUDIT | LOG

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that a GiGE port speed, auto-negotiation, and/or FEC Clause has changed.

ESM-2802

Message

Port <Port Name> protocol is set to <FCIP/LAN> [<App>].

Message Type

AUDIT | LOG

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that a GiGE port has been changed to FCIP/LAN.

ESM-2803

Message

Port <Port Name> channel ID is set to <channel ID> [<App>].

Message Type

AUDIT | LOG

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that a GiGE port channel id has changed.

ESM-3000**Message**

<Boot Stage> starting.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates the specific bootup recovery stage has started.

ESM-3001**Message**

<Boot Stage> complete.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates the specific bootup recovery stage has completed.

ESM-3002**Message**

DP<DP ID>-<HA Stage> starting.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates the specific HA recovery stage has started for the specified Data Processor (DP).

ESM-3003**Message**

DP<DP ID>-<HA Stage> ending: <Recovery Status>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates the specific HA recovery stage has completed for the specified Data Processor (DP).

ESM-3004**Message**

DP<DP ID> VE-<HA Operation> Tunnel <VE Port> failed (<Reason>). Will retry.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates the specific HA operation has failed for the specified VE port but will be retried later.

ESM-3005**Message**

DP<DP ID> VE-<HA Operation> Tunnel <VE Port> failed (<Reason>). Not retrievable.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates the specific HA operation has failed for the specified VE port and traffic will be disrupted on this port.

ESM-3006**Message**

<Boot Stage> failed (<Reason>).

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that a critical failure has occurred during the boot process..

Recommended Action

If the message persists, execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

ESM-3007**Message**

DP<DP ID> VE Tunnel <VE Port> <HA Operation>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates the status of the specified data processor (DP), virtual expansion (VE) port, and high availability (HA).

ESM-3008

Message

Standby CP has mismatched mode for slot <Slot>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates a synchronization problem between active and standby CPs for a blade mode configuration.

Recommended Action

Reboot the standby CP to synchronize the blade mode.

ESM-3100

Message

Extension Performance Monitor started: <Name>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates the specified extension performance monitor session has started.

ESM-3101

Message

Extension Performance Monitor completed: <Name>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates the specified extension performance monitor session has completed.

ESM-3102**Message**

Extension Performance Monitor stopped: <Name> (reason:<Reason>).

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates the specified extension performance monitor session has stopped before completing for the indicated reason.

ESM-3103**Message**

Extension Performance Monitor aborted: <Name> (reason:<Reason>).

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates the specified extension performance monitor session has been aborted before completing for the indicated reason.

ESM-3104**Message**

Extension Performance Monitor deleted <Count> logfile(s).

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates the extension performance monitor logfiles have been deleted from the active CP.

ESS Messages

Exchange Switch Support (ESS) error messages.

ESS-1001

Message

A few switches in the fabric do not support the Coordinated HotCode protocol.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates one or more switches in the fabric do not support the Coordinated HotCode protocol. Continuing with the firmware download may cause data traffic disruption.

Recommended Action

Discontinue the firmware download, identify the down-level switch or switches that do not support the Coordinated HotCode protocol, and upgrade the down-level switches. Then, restart the firmware download on this switch. Note that upgrading a down-level Brocade switch in a mixed interop fabric may still cause data traffic disruption.

ESS-1002

Message

The pause message is rejected by the domain <domain id>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that during the Coordinated HotCode protocol, a switch in the fabric has rejected the pause message which prevented the protocol from completing. Any data traffic disruption observed during the firmware download may have been due to the rejected pause message.

ESS-1003

Message

The pause retry count is exhausted for the domain <domain id>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that during the Coordinated HotCode protocol, a switch in the fabric did not accept the pause message which prevented the protocol from completing. Any data traffic disruption observed during the firmware download may have been due to this issue.

ESS-1004

Message

The resume message is rejected by the domain <domain id>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that during the Coordinated HotCode protocol, a switch in the fabric has rejected the resume message which prevented the protocol from completing. Any data traffic disruption observed during the firmware download may have been due to the rejected resume message.

ESS-1005

Message

The resume retry count is exhausted for the domain <domain id>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that during the Coordinated HotCode protocol, a switch in the fabric did not accept the resume message which prevented the protocol from completing. Any data traffic disruption observed during the firmware download may have been due to this issue.

ESS-1008**Message**

Fabric Name - <fabric_name> configured (received from domain <domain id>).

Message Type

AUDIT | LOG

Message Class

FABRIC

Message Severity

INFO

Probable Cause

Indicates that the fabric name is configured or renamed.

ESS-1009**Message**

Fabric Name Mismatch - local(<fabric_name>) remote(<r_fabric_name> - received from domain <domain id>).

Message Type

AUDIT | LOG

Message Class

FABRIC

Message Severity

WARNING

Probable Cause

Indicates that the specified fabric name is not unique for this fabric.

Recommended Action

Select an appropriate fabric name and set it again from any switch.

ESS-1010

Message

Duplicate Fabric Name - <fabric_name> matching with FID <Fabric ID>.

Message Type

AUDIT | LOG

Message Class

FABRIC

Message Severity

WARNING

Probable Cause

Indicates that the configured fabric name is already used for another partition.

Recommended Action

Select a different fabric name and reconfigure.

ESS-1011

Message

Unable to retrieve local Fabric Name configuration. Remote name <r_fabric_name> from domain <domain id>

Message Type

AUDIT | LOG

Message Class

FABRIC

Message Severity

WARNING

Probable Cause

Indicates that there has been a Fabric name configuration retrieval failure from local database which has resulted in Fabric Name from the specified remote domain to be inherited.

Recommended Action

Select an appropriate fabric name and set it again from local switch.

ESS-1012

Message

Invalid Physical port range capability data is received from domain <domain id>.

Message Type

LOGFFDC

Message Severity

WARNING

Probable Cause

Indicates that an invalid physical port range capability was received from a remote switch.

Recommended Action

If the problem persists, please contact your switch service provider for further investigation.

ESS-2001

Message

Fabric Hello Timeout: Inter-switch Frame Delivery problem - remote Switch Domain <Remote Domain>, port <Port>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates failure to send or receive frames to the specified remote switch domain even after several retry attempts. The following are the possible failure reasons:

- 7 - Routing Problem
- 14 - Reliable Transmit With Response (RTWR) send failure

Recommended Action

Check the status of fabric and the specified remote switch domain.

If the problem persists, execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

ESS-2002

Message

Recover from Fabric Hello Timeout - remote Switch domain <Remote Domain>, port <Port>, failure cnt <Failure Count>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates recovery from previously detected problem with sending frames to the specified remote switch domain.

ESW Messages

ESW error messages.

ESW-1001

Message

Switch is not in ready state - Switch enable failed, switch status= 0x<switch status>, c_flags = 0x<switch control flags>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the switch enable operation has failed.

Recommended Action

If the message persists, execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

ESW-1002

Message

Security violation: Unauthorized device <wwn name of device> tries to FLOGI to port <port number>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the specified device is not present in the authorized profile list.

Recommended Action

Verify that the device is authorized to log in to the switch. If the device is authorized, execute the `secPolicyDump` command to verify whether the World Wide Name (WWN) of the specified device is listed. If it is not listed, execute the `secPolicyAdd` command to add this device to an existing policy.

ESW-1003**Message**

Slot ENABLED but Not Ready during recovery, disabling slot = <slot number>(<return value>).

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the slot state has been detected as inconsistent during failover or recovery.

Recommended Action

For a bladed switch, execute the `slotPowerOff` and `slotPowerOn` commands to power cycle the blade.

For a non-bladed switch, restart or power cycle the switch.

ESW-1004**Message**

Blade attach failed during recovery, disabling slot = <slot number>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the specified blade has failed during failover or recovery.

Recommended Action

For a bladed switch, execute the `slotPowerOff` and `slotPowerOn` commands to power cycle the blade.

For a non-bladed switch, restart or power cycle the switch.

ESW-1005**Message**

Diag attach failed during recovery, disabling slot = <slot number>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the diagnostic blade attach operation has failed during failover or recovery.

Recommended Action

For a bladed switch, execute the `slotPowerOff` and `slotPowerOn` commands to power cycle the blade.

For a non-bladed switch, restart or power cycle the switch.

ESW-1006**Message**

HA state out of sync: Standby CP (ver = <standby SWC version>) does not support NPIV functionality. (active ver = <active SWC version>, NPIV devices = <'1' if NPIV devices exist; Otherwise '0'>).

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the standby control processor (CP) does not support N_Port ID Virtualization (NPIV) functionality, but the switch has some NPIV devices logged in to the fabric.

Recommended Action

Load a firmware version on the standby CP that supports NPIV functionality using the `firmwareDownload` command.

ESW-1007

Message

Switch port <port number> disabled due to \"<disable reason>\".

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the switch port is disabled due to the reason displayed in the message.

Recommended Action

Based on the disable reason displayed, take appropriate action to restore the port.

If the disable reason is "Insufficient frame buffers", reduce the distance or speed settings for the port to reduce the buffer requirement of the link. Alternatively, one or more ports in the port group must be disabled to make more buffers available for the link.

Refer to the *Fabric OS Administrator's Guide* for more information.

ESW-1008

Message

<area string> are port swapped on ports that do not support port swap. Slot <slot number> will be faulted.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the blade is enabled with the port configuration that already has the area swapped.

Recommended Action

Replace the blade with ports that support port swap. Then swap ports back to the port's default area.

Refer to the *Fabric OS Administrator's Guide* for more information.

EVMD Messages

EVMD is the event management module error messages.

EVMD-1001

Message

Event could not be sent to remote proxy = <Remote proxy switch id>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the event could not be sent to remote proxy. This could happen if the remote proxy switch cannot be reached through in-band.

Recommended Action

Make sure that the specified remote domain is present in the fabric.

EXDP Messages

Extension Date Path Processor error messages.

EXDP-1005

Message

Datapath Slot:<slot number> Chip:<Chip number> reset during HAreboot.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that a datapath chip reset happened during a high availability (HA) reboot. Traffic may be disrupted.

Recommended Action

Reboot to recover.

EXDP-1006

Message

Slot <Slot number>, Port <Port number>(<blade index>), DP <DP id>: Multi Frame Loss detected on internal port. VC_no: <vc number>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that frames/credits were lost on an internal port and the link must be reset to recovery.

Recommended Action

Turn on back-end credit recovery to reset the link and recover the lost credits. If credit recovery has already been turned on, the link will be reset to recover the credits and no action is required.

EXDP-1007

Message

Slot <Slot number>, Port <Port number>(<blade index>), DP <DP id>: Multi Ready Loss detected on internal port. VC_no: <vc number>, credits lost: <Credits lost>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that frames/credits were lost on an internal port and the link must be reset to recovery.

Recommended Action

Turn on the back-end credit recovery to reset the link and recover the lost credits. If credit recovery has already been turned on, the link will be reset to recover the credits and no action is required.

EXDP-1008

Message

Datapath Slot <slot number> Chip <Chip number>: fault received due to link level CRC errors on internal port.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that CRC errors were received on an internal port of the datapath chip.

Recommended Action

Contact your equipment vendor's support.

FABR Messages

FABR error messages come from the fabric daemon.

FABR-1001

Message

port <port number>, <segmentation reason>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the specified switch port is isolated because of a segmentation resulting from mismatched configuration parameters.

Recommended Action

Based on the segmentation reason displayed with the message, look for a possible mismatch of relevant configuration parameters in the switches at both ends of the link.

Run the `configure` command to modify the appropriate switch parameters on both the local and remote switch.

FABR-1002

Message

fabGaid: no free multicast alias IDs.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the fabric does not have any available multicast alias IDs to assign to the alias server.

Recommended Action

Verify alias IDs using the `fabricShow` command on the principal switch.

FABR-1003**Message**

port <port number>: ILS <command> bad size <payload size>, wanted <expected payload size>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that an internal link service (ILS) information unit of invalid size has been received. The neighbor switch has sent a payload with an invalid size.

Recommended Action

Investigate the neighbor switch for problems. Run the `errShow` command on the neighbor switch to view the error log for additional messages.

Check for a faulty cable or deteriorated small form-factor pluggable (SFP). Replace the cable or the SFP if necessary.

Run the `portLogDumpPort` command on both the receiving and transmitting ports.

Run the `fabStatsShow` command on both the receiving and transmitting switches.

If the message persists, run the `supportFtp` command (as needed) to set up automatic FTP transfers; then run the `supportSave` command and contact your switch service provider.

FABR-1004**Message**

port: <port number>, req iu: 0x<address of IU request sent>, state: 0x<command sent>, resp iu: 0x<address of response IU received>, state 0x<response IU state>, <additional description>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the information unit response was invalid for the specified command sent. The fabric received an unknown response. This message is rare and usually indicates a problem with the Fabric OS kernel.

Recommended Action

If this message is due to a one-time event because of the incoming data, the system will discard the frame. If it is due to problems with the kernel, the system will recover by performing a failover.

If the message persists, run the `supportFtp` command (as needed) to set up automatic FTP transfers; then run the `supportSave` command and contact your switch service provider.

FABR-1005**Message**

<command sent>: port <port number>: status 0x<reason for failure> (<description of failure reason>) xid = 0x<exchange ID of command>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the application failed to send an async command for the specified port. The message provides additional details regarding the reason for the failure and the exchange ID of the command. This can happen if a port is about to go down.

Recommended Action

This message is often transitory.

If the message persists, run the `supportFtp` command (as needed) to set up automatic FTP transfers; then run the `supportSave` command and contact your switch service provider.

FABR-1006**Message**

Node free error, caller: <error description>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the Fabric OS is trying to free or deallocate memory space that has already been deallocated. This message is rare and usually indicates a problem with the Fabric OS.

Recommended Action

In case of severe memory corruption, the system may recover by performing an automatic failover.

If the message persists, run the `supportFtp` command (as needed) to set up automatic FTP transfers; then run the `supportSave` command and contact your switch service provider.

FABR-1007**Message**

IU free error, caller: <function attempting to de-allocate IU>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that a failure occurred when deallocating an information unit. This message is rare and usually indicates a problem with the Fabric OS.

Recommended Action

In case of severe memory corruption, the system may recover by performing an automatic failover.

If the message persists, run the `supportFtp` command (as needed) to set up automatic FTP transfers; then run the `supportSave` command and contact your switch service provider.

FABR-1008**Message**

<error description>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that errors occurred during the request domain ID state; the information unit cannot be allocated or sent. If this message occurs with FABR-1005, the problem is usually transitory. Otherwise, this message is rare and usually indicates a problem with the Fabric OS. The error descriptions are as follows:

- FAB RDI: cannot allocate IU
- FAB RDI: cannot send IU

Recommended Action

If the message appears with the FABR-1005 message.

If the message persists, run the `supportFtp` command (as needed) to set up automatic FTP transfers; then run the `supportSave` command and contact your switch service provider.

FABR-1009**Message**

<error description>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that errors were reported during the exchange fabric parameter state; cannot allocate domain list due to a faulty exchange fabric parameter (EFP) type. This message is rare and usually indicates a problem with the Fabric OS.

Recommended Action

The fabric daemon will discard the EFP. The system will recover through the EFP retrieval process.

If the message persists, run the `supportFtp` command (as needed) to set up automatic FTP transfers; then run the `supportSave` command and contact your switch service provider.

FABR-1010**Message**

<error description>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that errors occurred while cleaning up the request domain ID (RDI). The error description provides further details. This message is rare and usually indicates a problem with the Fabric OS.

Recommended Action

If the message persists, run the `supportFtp` command (as needed) to set up automatic FTP transfers; then run the `supportSave` command and contact your switch service provider.

FABR-1011**Message**

<error description>.

Message Type

LOG | FFDC

Message Severity

ERROR

Probable Cause

Indicates that the Fabric OS is unable to inform the Fabric OS State Synchronization Management module (FSSME) that the fabric is stable or unstable. This message is rare and usually indicates a problem with the Fabric OS.

Recommended Action

If the message persists, run the `supportFtp` command (as needed) to set up automatic FTP transfers; then run the `supportSave` command and contact your switch service provider.

FABR-1012**Message**

<error description>:State <switch or port state>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the fabric is not in the appropriate state for the specified process. This message is rare and usually indicates a problem with the Fabric OS.

Recommended Action

The fabric daemon will take proper action to recover from the error.

If the message persists, run the `supportFtp` command (as needed) to set up automatic FTP transfers; then run the `supportSave` command and contact your switch service provider.

FABR-1013**Message**

No Memory: pid=<fabric process id> file=<source file name> line=<line number within the source file>.

Message Type

FFDC | LOG

Message Severity

CRITICAL

Probable Cause

Indicates that there is not enough memory in the switch for the fabric module to allocate. This message is rare and usually indicates a problem with the Fabric OS.

Recommended Action

The system will recover by failing over to the standby CP.

If the message persists, run the `supportFtp` command (as needed) to set up automatic FTP transfers; then run the `supportSave` command and contact your switch service provider.

FABR-1014**Message**

Port <port number> Disabled: Insistent Domain ID <Domain ID> could not be obtained. Principal Assigned Domain ID = <Domain ID>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the specified port received a request domain ID (RDI) accept message containing a principal-switch-assigned domain ID that is different from the insistent domain ID (IDID). Fibre connectivity (FICON) mode requires an insistent domain ID. If an RDI response has a different domain ID, then the port is disabled.

Recommended Action

Run the `configShow` command to view the `fabric.ididmode`. A 0 means the IDID mode is disabled; a 1 means it is enabled.

Set the switch to insistent domain ID mode. This mode is set under the `configure` command or in Web Tools on the **Switch Admin > Configure** window.

FABR-1015**Message**

FICON Insistent DID max retry exceeded: All E_Ports will be disabled. Switch is isolated.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the application exceeded request domain ID (RDI) requests for the insistent domain ID. All E_Ports are disabled; isolating the specified switch from the fabric.

Recommended Action

Verify that the insistent domain ID is unique in the fabric and then re-enable the AE_Ports. Run the `fabricShow` command to view the domain IDs across the fabric and the `configure` command to change the insistent domain ID mode. Refer to the *Brocade Analytics Monitoring Platform Command Reference* for more information on these commands.

FABR-1016**Message**

ficonMode is enabled.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that FICON mode is enabled on the switch through a user interface command.

FABR-1017

Message

ficonMode is disabled.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that FICON mode is disabled on the switch through a user interface command.

FABR-1018

Message

Loss in fabric principal status during principal switch selection phase of fabric reconfiguration (<reason for not becoming the principal switch>: <WWN of new principal switch>).

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that a failure occurred when trying to set the principal switch using the `fabricPrincipal` command. The message notifies you that the switch failed to become the principal switch because of one of the following reasons:

- The switch joined an existing fabric and bypassed the F0 state.
- The fabric already contains a principal switch that has a lower World Wide Name (WWN).

Recommended Action

Make sure that no other switch is configured as the principal switch. Force a fabric rebuild by using the `switchDisable` and `switchEnable` commands.

Refer to the *Brocade Analytics Monitoring Platform Command Reference* for more information about the `fabricPrincipal` command.

FABR-1019

Message

Critical fabric size (<current domains>) exceeds supported configuration (<supported domains>).

Message Type

FFDC | LOG

Message Severity

CRITICAL

Probable Cause

Indicates that this switch is a value-line switch and has exceeded the limited fabric size: that is, a specified limit to the number of domains. This limit is defined by your specific value-line license key. The fabric size has exceeded this specified limit, and the grace period counter has started. If the grace period is complete and the size of the fabric is still outside the specified limit, Web Tools is disabled.

Recommended Action

Bring the fabric size within the licensed limits. Either a full fabric license must be added or the size of the fabric must be changed to within the licensed limit. Contact your switch provider to obtain a full fabric license.

FABR-1020**Message**

Web Tools will be disabled in <days> days <hours> hours and <minutes> minutes.

Message Type

FFDC | LOG

Message Severity

CRITICAL

Probable Cause

Indicates that this switch has a value-line license and has a limited number of domains. If more than the specified number of domains are in the fabric, a counter is started to disable Web Tools. This message displays the number of days left in the grace period. After this time, Web Tools is disabled.

Recommended Action

Bring the fabric size within the licensed limits. Either a full fabric license must be added or the size of the fabric must be changed to within the licensed limit. Contact your switch provider to obtain a full fabric license.

FABR-1021**Message**

Web Tools is disabled.

Message Type

FFDC | LOG

Message Severity

CRITICAL

Probable Cause

Indicates that this switch has a value-line license and has a limited number of domains. If more than the specified number of domains are in the fabric, a counter is started to disable Web Tools. This grace period has expired and Web Tools has been disabled.

Recommended Action

Bring the fabric size within the licensed limits. Either a full fabric license must be added or the size of the fabric must be changed to within the licensed limit. Contact your switch provider to obtain a full fabric license.

FABR-1022**Message**

Fabric size (<actual domains>) exceeds supported configuration (<supported domains>). Fabric limit timer (<type>) started from <grace period in seconds>.

Message Type

FFDC | LOG

Message Severity

CRITICAL

Probable Cause

Indicates that the fabric size has exceeded the value-line limit, and the grace period counter has started. If the grace period is complete and the size of the fabric is still outside the specified limit, Web Tools is disabled.

Recommended Action

Bring the fabric size within the licensed limits. Either a full fabric license must be added or the size of the fabric must be changed to within the licensed limit. Contact your switch provider to obtain a full fabric license.

FABR-1023**Message**

Fabric size is within supported configuration (<supporteddomains>). Fabric limit timer (<type>) stopped at <grace period in seconds>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the fabric size is within specified limits. Either a full fabric license was added or the size of the fabric was changed to within the licensed limit.

FABR-1024**Message**

Initializing fabric size limit timer <grace period>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the fabric size has exceeded the limit set by your value-line switches. Value-line switches have a limited fabric size (for example, a specified limit on the number of domains). This value is defined by your specific value-line license key. The fabric size has exceeded this specified limit. The grace period timer has been initialized. If the grace period is complete and the size of the fabric is still outside the specified limit, Web Tools is disabled.

Recommended Action

Bring the fabric size within the licensed limits. Either a full fabric license must be added or the size of the fabric must be changed to within the licensed limit. Contact your switch provider to obtain a full fabric license.

FABR-1029**Message**

Port <port number> negotiated <flow control mode description> (mode = <received flow control mode>).

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that a different flow control mode, as described in the message, is negotiated with the port at the other end of the link. The flow control is a mechanism of throttling the transmitter port to avoid buffer overrun at the receiving port. There are three types of flow control modes:

- VC_RDY mode: Virtual-channel flow control mode. This is a proprietary protocol.
- R_RDY mode: Receiver-ready flow control mode. This is the Fibre Channel standard protocol, that uses R_RDY primitive for flow control.
- DUAL_CR mode: Dual-credit flow control mode. In both of the previous modes, the buffer credits are fixed, based on the port configuration information. In this mode, the buffer credits are negotiated as part of exchange link parameter (ELP) exchange. This mode also uses the R_RDY primitive for flow control.

FABR-1030

Message

fabric: Domain <new domain ID> (was <old domain ID>).

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the domain ID has changed.

FABR-1031

Message

Maximum number of retries sending ILS from port <port number> exceeded.

Message Type

LOG | FFDC

Message Severity

WARNING

Probable Cause

Indicates the fabric exhausted the maximum number of retries sending internal link service (ILS) to the iswitch daemon on the specified E_Port.

Recommended Action

Run the `top` command to see if iswitchd is extremely busy or if another process is using excessive CPU resources.

FABR-1032

Message

Remote switch with domain ID <Domain ID> and switchname <Switchname> running an unsupported FOS version v2.x has joined the fabric.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that a switch with an unsupported Fabric OS version 2.x has joined the fabric.

Recommended Action

Remove the switch with the unsupported Fabric OS version 2.x from the fabric

FABR-1034

Message

Area <Area that has already been acquired> have been acquired by port <Port that has already acquired the area>. Persistently disabling port <Port that is being disabled>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates you must enable Trunk Area on a port for another port to use the same area.

Recommended Action

Move the cable to a port area that is not in use, or disable Trunk Area. You must manually enable the port or the port remains disabled forever.

Refer to the *Fabric OS Administrator's Guide* for more information.

FABR-1035

Message

Slave area <Area that does not match Master port's area> does not match Master port <Master port >. Persistently disabling port <Port that is being disabled>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates the Slave port's Trunk Area differs from that of the Master port.

Recommended Action

Move the cable to a port to match with the same Master Trunk Area, or disable Trunk Area. You must manually enable the port or the port remains disabled forever.

Refer to the *Fabric OS Administrator's Guide* for more information.

FABR-1036

Message

F_Port trunks are only allowed on Trunk Area enabled port. Persistently disabling port <Port that is being disabled>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates the specified port is being disabled because when the port on a switch is Trunk Area-enabled, it does not allow other devices like Access Gateway (AG) or HBA that are not Trunk Area-enabled.

Recommended Action

Move the cable to a port that does not have Trunk Area enabled.

FABR-1037

Message

Port configuration incompatible with Trunk Area enabled port. Persistently disabling port <Port that is being disabled>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates the specified port is being disabled because when the port attempts to go online, the switch finds the Trunk Area enabled is incompatible with port configurations such as long distance, port mirror, fast write, or EX_Port.

Recommended Action

Check the port configurations to disable long distance, port mirror, fast write, or EX_Port.

FABR-1038**Message**

Trunking license not present with F port trunking enabled. Persistently disabling port <Port that is being disabled>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates the specified port is being disabled because F_Port trunking is enabled without a trunking license being present.

Recommended Action

Install a trunking license or disable F_Port trunking on the port.

FABR-1039**Message**

Invalid domain ID zero received from principal switch(domain id=<Principal domain id>).

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates an invalid domain ID zero has been received.

Recommended Action

Check the principal switch for the invalid domain ID zero.

FABR-1040**Message**

Speed is not 2G, 4G, or 8G with F_Port trunking enabled. Persistently disabling port <Port that is being disabled>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the speed is not compatible for F_Port trunks.

Recommended Action

Change the speed for the port or disable F_Port trunking on the port.

FABR-1041**Message**

Port <Port that is being disabled> is disabled due to trunk protocol error.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates a link reset was received before the completion of the trunking protocol on the port.

Recommended Action

Enable the port by running the `portEnable` command.

The port may recover by re-initialization of the link.

If the message persists, run the `supportFtp` command (as needed) to set up automatic FTP transfers; then run the `supportSave` command and contact your switch service provider.

FABR-1043

Message

Detected Fabric ID conflict with remote (not neighbor) switch <Switchname> (domain <Domain ID>), FID <Fabric ID>. No local E_Ports disabled.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the remote switch has a Fabric ID (FID) conflict with the local switch. But no ports are disabled because the remote switch is not an adjacent to the local switch.

Recommended Action

Make sure that all the switches in the fabric have the same FID or upgrade the switch firmware to a VF-capable firmware.

FABR-1044

Message

Detected Fabric ID conflict with neighbor switch <Switchname> (domain <Domain ID>), FID <Fabric ID>. E_Ports (<Number of E_Ports disabled>) connected to the switch are disabled.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the neighbor switch has a Fabric ID (FID) conflict with the local switch. All E_Ports directly connected to the conflicting switch are disabled.

Recommended Action

Make sure that all the switches in the fabric have the same FID or upgrade the switch firmware to a VF-capable firmware.

FABR-1045

Message

Detected Base Switch conflict with remote (not neighbor) switch <Switchname> (domain <Domain ID>), BS <Base Switch Mode>. No local E_Ports disabled.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the remote switch has a Base Switch attribute conflict with the local switch. But no ports are disabled because the remote switch is not an adjacent to the local switch.

Recommended Action

Make sure that all the switches in the fabric have the same Base Switch attribute or disable VF mode for the conflicting switch using the `fosconfig --disable vf` command.

FABR-1046**Message**

Detected Base Switch conflict with neighbor switch <Switchname> (domain <Domain ID>), BS <Base Switch Mode>. E_Ports (<Number of E_Ports disabled>) connected to the switch are disabled.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the remote switch has a Base Switch attribute conflict with the local switch. All the E_Ports directly connected to the conflicting switch are disabled.

Recommended Action

Make sure that all the switches in the fabric have the same Base Switch attribute or upgrade the switch firmware to a VF-capable firmware.

FABR-1047**Message**

Area unavailable to assign to the port. Persistently disabling port <Port that is being disabled>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that there are no areas available to assign to the port during port creation.

Recommended Action

Move some ports out of the default switch to make areas available.

FABR-1048**Message**

Detected Fabric ID (FID <InheritedFID> inherited) conflict with switch <Switchname> (domain <Domain ID>, FID <Fabric ID>).

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that a switch in the fabric has a Fabric ID (FID) conflict with the inherited FID of the local switch.

Recommended Action

Make sure that all the switches in the fabric have the same FID or upgrade the switch firmware to a VF-capable firmware.

FABR-1049**Message**

Detected Fabric ID (FID <InheritedFID> inherited) conflict with neighbor switch <Switchname> (domain <Domain ID>, FID <Fabric ID>). E_Ports (<Number of E_Ports disabled>) connected to the switch are disabled.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the neighbor switch has a Fabric ID (FID) conflict with the inherited FID of the local switch. All E_Ports directly connected to the conflicting switch are disabled.

Recommended Action

Make sure that all the switches in the fabric have the same FID or upgrade the switch firmware to a VF-capable firmware.

FABR-1050**Message**

<License> license not present. F_Port trunking cannot be enabled on port(<Port>).

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the trunking or Server Application Optimization (SAO) license is not installed.

Recommended Action

Install the license required.

FABR-1051**Message**

D-Port <Testname> test failed for slot <Slot> and port <Port>.

Message Type

LOG | AUDIT

Message Class

FABRIC

Message Severity

ERROR

Probable Cause

Indicates that the D_Port test failed for the given slot and port due to one of the following reasons:

- The small form-factor pluggable (SFP) fault detected by electrical loopback test failure.
- The cable fault detected by optical loopback test failure.
- An application-specific integrated circuit (ASIC) issue detected by link traffic test failure.

Recommended Action

Replace the faulty SFPs, cables, or blade.

FABR-1052

Message

The configured port speed is invalid. Persistently disabling port <Port that is being disabled>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the configured speed for the specified port is invalid.

Recommended Action

Execute the `portCfgSpeed` command to change the port speed.

FABR-1053

Message

The switch is disabled due to an inconsistency found in the interop config parameters.

Message Type

LOG

Message Severity

CRITICAL

Probable Cause

Indicates that the configuration keys have interopmode parameters such as `switch.interopMode` and `switch.mcdtFabricmode` set.

Recommended Action

Execute the `interopmode` command to reset the parameters.

FABR-1054

Message

Rebooting the standby as it received an update before port [<Port Number>] is expanded.

Message Type

LOG | FFDC

Message Severity

INFO

Probable Cause

Indicates that the standby control processor (CP) did not have the port because the port expand operation is still in progress and the standby CP has received a port update. The standby CP reboots automatically to ensure sync and attain the normal state. This is a rare occurrence.

FABR-1055**Message**

F_Port trunking cannot be enabled on the slot <Slot Number> port <Port Number> due to inconsistent port configuration.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the specified F_Port is unable to join its assigned trunk area group because of mismatch in the port configuration with the other trunk area members.

Recommended Action

Check the configuration of the port with all other ports intended to be part of the same trunk group. Use the `porttrunkarea --show` to identify the trunk members of the specified F_Port and the `portcfgshow` command to identify the conflicting configuration between the trunk members.

FABR-1056**Message**

Check trunking license validity and trunk port configuration on remote switch. Persistently disabling port <Port that is being disabled>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the specified port on a trunk area-enabled switch is being disabled. Make sure that the remote switch such as Access Gateway (AG) or Host Bus Adapter (HBA) device has the valid trunking license and trunk port configuration.

Recommended Action

Install trunking license and enable trunk port configuration on the remote switch.

FABR-1057**Message**

Failed to set default domain for AMP switch

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the failure happened when trying to set default domain (150) for AMP switch.

Recommended Action

Collect supportsave using the `supportsave` command.

FABR-1058**Message**

Failed to set default principal switch priority for AMP switch

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the failure happened when trying to set default principal switch priority (0xFF) for AMP switch.

Recommended Action

Collect supportsave using the `supportsave` command.

FABR-1059**Message**

Detected local Domain ID change from <Old Domain ID> to <New Domain ID>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the local domain ID is changed while the switch is still online, all the devices are logged out, and the switch is in an inconsistent state. An automatic switch toggle happens along with this raslog message to recover the switch if the standby CP runs FOS v8.2.0 or later.

Recommended Action

To make the new domain ID effective, an automatic **switchdisable** followed by **switchenable** is performed if the standby CP runs the FOS v8.2.0 or later. Otherwise, perform **switchdisable** followed by **switchenable**. This can be a disruptive operation.

If the message persists, run the `supportFtp` command (as needed) to set up automatic FTP transfers; then run the `supportSave` command and contact your switch service provider.

FABR-1060**Message**

Detected local Domain ID change from <Old Domain ID> to <New Domain ID>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the local domain ID is changed while the switch is still online and the switch is in inconsistent state. Toggle the switch manually along with raslog message to recover the switch if the standby CP runs FOS earlier to v8.2.0.

Recommended Action

To make the new domain ID effective, the user has to do a **switchdisable** followed by a **switchenable**. This can be a disruptive operation.

If the message persists, run the `supportFtp` command (as needed) to set up automatic FTP transfers; then run the `supportSave` command and contact your switch service provider.

FABR-1061**Message**

F-Port trunking is not supported with the HBA on this platform. Persistently disabling port <Port that is being disabled>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the specified port on a trunk area-enabled switch is being disabled. Make sure that the remote Host Bus Adapter (HBA) device is supported with this platform.

Recommended Action

Connect HBA supported with this platform and enable the port

FABR-1062**Message**

Fabric reconfiguration triggered in the fabric

Message Type

AUDIT

Message Class

FABRIC

Message Severity

INFO

Probable Cause

User has initiated build fabric operation in the current fabric.

FABR-1063**Message**

IDID <Domain ID> could not be obtained. To obtain the IDID, disable PDID feature on principal switch and enable IDID conflict ports.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the specified port received a request domain ID (RDI) accept message containing a principal-switch-assigned domain ID that is different from the insistent domain ID (IDID). Fibre connectivity (FICON) mode requires an insistent domain ID. If an RDI response has a different domain ID, then the port is disabled.

Recommended Action

Run the `configure` command on principal switch to verify the configuration parameter "Disable Preserved Domain ID Mode". It will show whether the Preserved Domain ID feature is enabled or not.

Disable Preserved Domain ID allocation feature in the principal switch and enable it again once the new switch joins the fabric successfully. This feature is seen under the `configure` command or in Web Tools on the **Switch Admin > Configure** window.

FABR-1064**Message**

Port <Port>, Requested DID <Requested Domain ID>, Allocated DID <Allocated Domain ID>. To allocate requested DID, disable PDID feature on the principal switch if enabled.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the specified port received a request domain ID (RDI) accept message containing a principal-switch-assigned domain ID that is different from the insistent domain ID (IDID). Fibre connectivity (FICON) mode requires an insistent domain ID. If an RDI response has a different domain ID, then the port is disabled.

Recommended Action

Run the `configure` command on principal switch to verify the configuration parameter "Disable Persistent Domain ID Mode". It will show whether the Preserved Domain ID feature is enabled or not.

Disable Preserved Domain ID allocation feature in the principal switch and enable it again once the new switch joins the fabric successfully. This feature is seen under the `configure` command or in Web Tools on the **Switch Admin > Configure** window.

FABR-1065**Message**

Trunk area configuration restore failed for port <Port> due to <Failure reason>

Message Type

LOG

Message Severity

ERROR

Probable Cause

Trunk area configuration could not be restored

Recommended Action

Manually enable the trunk area configuration for the port

FABR-1066**Message**

Trunk area configuration save failed for port <Port> due to <Failure reason>

Message Type

LOG

Message Severity

INFO

Probable Cause

Trunk area configuration could not be saved

Recommended Action

Action has to be taken as per the failure reason provided

FABR-1067**Message**

No trunk port members are found for trunk area index <Trunk area index>, so trunk area configuration is skipped

Message Type

LOG

Message Severity

ERROR

Probable Cause

Existing trunk group members have been moved to a different trunk area index

Recommended Action

Manually reconfigure the trunk area for the port

FABR-3000

Message

D-Port test <Start, Restart or Stop D-Port request> request initiated for <Port/Ports for which the D-Port test request initiated>

Message Type

AUDIT

Message Class

FABRIC

Message Severity

INFO

Probable Cause

User has either started, restarted or stopped D-Port test on specific port

FABS Messages

Fabric OS system driver module error messages.

FABS-1001

Message

<Function name> <Description of memory need>.

Message Type

FFDC | LOG

Message Severity

CRITICAL

Probable Cause

Indicates that the system is low on memory and cannot allocate more memory for new operations. This is usually an internal Fabric OS problem or file corruption. The *Description of memory need* variable specifies the memory size that was being requested. The value can be any whole number.

Recommended Action

Reboot or power cycle the switch.

FABS-1002

Message

<Function name> <Description of problem>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that an internal problem has been detected by the software. This is usually an internal Fabric OS problem or file corruption.

Recommended Action

Reboot or power cycle the switch.

If the message persists, run the `firmwareDownload` command to update the firmware.

FABS-1004

Message

<Function name and description of problem> process <Process ID number> (<Current command name>) <Pending signal number>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that an operation has been interrupted by a signal. This is usually an internal Fabric OS problem or file corruption.

Recommended Action

Reboot or power cycle the switch.

FABS-1005

Message

<Function name and description of problem> (<ID type>= <ID number>).

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that an unsupported operation has been requested. This is usually an internal Fabric OS problem or file corruption. The following is a possible value for *function name and description of problem* variable:

fabsys_write: Unsupported write operation: process xxx

In this value, xxx is the process ID (PID), which could be any whole number.

Recommended Action

Reboot or power cycle the active CP (for modular systems) or the switch (for single-board systems).

If the message persists, run the `firmwareDownload` command to update the firmware.

FABS-1006**Message**

<Function name and description of problem>: object <object type id> unit <slot>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that there is no device in the slot with the specified object type ID in the system module record. This could indicate a serious Fabric OS data problem on the switch. The possible values for *function name and description of problem* variable are:

- setSoftState: bad object
- setSoftState: invalid type or unit
- media_sync: Media oid mapping failed
- fabsys_media_i2c_op: Media oid mapping failed
- fabsys_media_i2c_op: obj is not media type
- media_class_hdlr: failed sending media state to blade driver

Recommended Action

If the message is isolated, monitor the error messages on the switch. If the error is repetitive or if the fabric failed, failover or reboot the switch.

If the message persists, run the `firmwareDownload` command to update the firmware.

FABS-1007

Message

<Function name>: Media state is invalid - status=<Status value>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the Fabric OS has detected an invalid value in an object status field. This is usually an internal Fabric OS problem or file corruption.

Recommended Action

Reboot or power cycle the switch.

If the message persists, run the `firmwareDownload` command to update the firmware.

FABS-1008

Message

<Function name>: Media oid mapping failed.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the Fabric OS was unable to locate a necessary object handle. This is usually an internal Fabric OS problem or file corruption.

Recommended Action

Reboot or power cycle the switch.

FABS-1009

Message

<Function name>: type is not media.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the Fabric OS was unable to locate an appropriate object handle. This is usually an internal Fabric OS problem or file corruption.

Recommended Action

Reboot or power cycle the switch.

FABS-1010**Message**

<Function name>: Wrong media_event <Event number>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the Fabric OS detected an unknown event type. This is usually an internal Fabric OS problem or file corruption.

Recommended Action

Reboot or power cycle the switch.

If the message persists, run the `firmwareDownload` command to update the firmware.

FABS-1011**Message**

<Method name>[0x<Method tag number>]:Invalid input state 0x<Input state code>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that an unrecognized state code was used in an internal Fabric OS message for a field-replaceable unit (FRU).

Recommended Action

Reboot or power cycle the CP or system.

If the message persists, run the `firmwareDownload` command to update the firmware.

FABS-1013**Message**

<Method name>[0x<Method tag number>]:Unknown blade type 0x<Blade type>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates an unrecognized type of blade has been discovered in the system.

This may be caused by an incorrect field-replaceable unit (FRU) header, inability to read the FRU header, or the blade may not be supported by this platform or Fabric OS version.

Recommended Action

Verify that the blade is valid for use in this system and this version of Fabric OS.

Reseat the blade.

If this is a valid blade and reseating does not solve the problem, replace the blade.

FABS-1014**Message**

<Method name>[0x<Method tag number>]:Unknown FRU type 0x<FRU Object type>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates an unrecognized type of field-replaceable unit (FRU) has been discovered in the system.

This may be caused by an incorrect FRU header, inability to read the FRU header, or the FRU may not be supported by this platform or Fabric OS version.

Recommended Action

Verify that the FRU is valid for use in this system and this version of Fabric OS.

Reseat the FRU.

If this is a valid FRU and reseating does not solve the problem, replace the FRU

FABS-1015

Message

<Method name>[0x<Method tag number>]:Request to enable FRU type 0x<FRU Object type>, unit <Unit number> failed.
err code <Error code>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates the specified FRU could not be enabled. This is usually an internal Fabric OS problem.

Recommended Action

Remove and reinsert the FRU.

Reboot or power cycle the CP or system.

If the message persists, run the `firmwareDownload` command to update the firmware.

FBC Messages

Firmware blade compatibility errors with the control processor (CP).

FBC-1001

Message

Firmware version on AP blade is incompatible with that on the CP.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates the control processor (CP) blade determined that the firmware version running on the application processor (AP) blade is not compatible with that running on CP. The AP and CP blades cannot communicate.

Recommended Action

The problem can be corrected by changing the firmware version on either the CP or on the AP blade. You can modify the firmware version on the CP blade by using the `firmwareDownload` command. Refer to the release notes to determine whether a non-disruptive firmware download is supported between the revisions. Because the AP and CP blades cannot communicate, it is not possible to load new firmware on the AP blade. If necessary, send the AP blade back to the factory for a firmware update.

FCLG Messages

Fibre Channel Link Aggregation (FC-LAG) error messages.

FCLG-1001

Message

FC-LAG port received initial FLOGI from non-Cisco WWN.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates FC-LAG port configuration/connection error.

Recommended Action

Check the FC-LAG port configuration/connection.

FCMC Messages

Fibre Channel miscellaneous messages.

FCMC-1001

Message

System is low on memory and has failed to allocate new memory.

Message Type

FFDC | LOG

Message Severity

CRITICAL

Probable Cause

Indicates that the switch is low on memory and failed to allocate new memory for an information unit (IU).

Recommended Action

A non-bladed switch will automatically reboot. For a bladed switch, the active CP blade will automatically fail over and the standby CP will become the active CP.

FCOE Messages

FCOE error messages.

FCOE-1001

Message

malloc failed for <Message>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates a memory allocation failure.

Recommended Action

Check the memory usage on the switch using the `memShow` command. Execute the `supportsave` and contact customer support.

FCOE-1002

Message

Max loggingroup limit reached at <limit>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that too many login groups have been added.

Recommended Action

Check the maximum login group value displayed in the message.

FCOE-1003**Message**

<device>: member in another loggingroup <lg> being removed.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the device World Wide Name (WWN) you are trying to add is present in some other login group, and therefore it will be removed from that login group and added to the new login group.

Recommended Action

Check the login group changes using the `fcoelogincfg --show` command.

FCOE-1004**Message**

<device>: removing member from <lg> failed.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that removing a device from the login group has failed.

Recommended Action

Execute the `supportSave` command and restart the system. If the problem persists, contact your switch service provider.

FCOE-1005

Message

<device>: membership check failed in loggingroup: <lg>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the membership check for the device has failed.

Recommended Action

Check the device for failed membership using the `fcoelogincfg --show` command.

FCOE-1006

Message

file operation failed on <filename> for <operation> operation: errno:<error>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates a file operation failure.

Recommended Action

Check the error code for the file operation failure and contact your switch service provider for assistance.

FCOE-1007

Message

Rejecting new FCoE login from interface <Interface info> [MAC <Device MAC>] due to duplicate Port WWN [<Port WWN>] with interface <Interface info> [pid:<Device PID>, MAC <Device MAC>].

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the specified new FCoE login has the same Port World Wide Name (PWWN) as an existing FCoE login.

Recommended Action

Check if the new FCoE device login is intended. If so, manually remove the old FCoE login using `fcoe --clear -login`.

FCOE-1008**Message**

Rejecting new FCoE NPIV login from interface <Interface info> [MAC <Device MAC>] due to duplicate Port WWN [<Port WWN>] with interface <Interface info> [pid:<Device PID>, MAC <Device MAC>].

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the specified new FCoE N_Port ID virtualization (NPIV) login has the same Port World Wide Name (PWWN) as an existing FCoE login.

Recommended Action

Check if the new FCoE NPIV login is intended. If so, manually remove the old FCoE login using `fcoe --clear -login`.

FCOE-1009**Message**

Addition of N_Port mapping failed. Max N_Port mapping limit reached: <max n_port>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the N_Port mapping has reached its maximum limit.

Recommended Action

Remove unwanted N_Port mappings using the `fcoelogingroup --remove` command and try adding N_Port mapping using the `fcoelogingroup --add` command.

FCOE-1010**Message**

fcoed: FSS Registration or Trace initialization failed.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the Fabric OS state synchronization (FSS) registration or initialization of the FCoE trace has failed.

Recommended Action

Execute the `supportSave` command and restart the system. If the problem persists, contact your switch service provider.

FCOE-1011**Message**

<Message>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates an error.

Recommended Action

Execute the `supportsave` and contact customer support.

FCOE-1019**Message**

FLOGI ignored as FCMAP is not configured on FCoE VLAN.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that FCMAP has not been configured on FCoE VLAN.

Recommended Action

Configure FCMAP on the FCoE VLAN using the `fcoe --fcmaset` command.

FCOE-1022**Message**

Login from interface <Interface info> [WWN <Device WWN>] failed. Max. FCoE device login limit [<Max. device limit>] reached.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the switch has reached its maximum allowed FCoE device limit. Hence the new device cannot be logged in

Recommended Action

Do not add any more FCoE devices to the switch.

FCOE-1023**Message**

Too many logins on FCoE VF_Port <FCoE VF_Port number> [WWN <Device WWN>, interface <Interface info>]; max allowed <Max. device limit per VF-Port>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the VF-Port has reached its maximum allowed FCoE login limit.

Recommended Action

If possible logout some of the logged-in devices using the `portdisable>` or `fcoe --clear -login` command and then log in the new device. You can view the list of logged-in devices using the `fcoe --show -login` command.

FCOE-1024**Message**

Received FDISC from interface <Interface info> [Enode MAC <Enode MAC>] without prior FLOGI.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that a FDISC frame is received from the end node that has not logged in. The end node must send a fabric login (FLOGI) before it can send an FDISC. This may be due to a CNA or target driver issue.

Recommended Action

Contact CNA or Target driver support team for assistance.

FCOE-1029**Message**

FIP version mismatch between FDISC [version <FDISC FIP version>, Port WWN <FDISC Device Port WWN>] and Base VN_Port login [version <Base VN_Port (FLOGI) FIP version>, MAC <Base VN_Port MAC>].

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates a FIP version mismatch between the fabric login (FLOGI) and FDISC device. This may be due to a CNA or Target driver issue.

Recommended Action

Contact CNA or Target driver support team for assistance.

FCOE-1030

Message

FIP version mismatch between FIP LOGO [version <FIP LOGO version>, WWN <Device WWN>] and Base VN_Port login [version <Base VN_Port (FLOGI) FIP version>, MAC <Base VN_Port MAC>].

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates a FIP version mismatch between the FCoE initialization protocol (FIP) logout and the base fabric login (FLOGI). This may be due to a CNA or Target driver issue.

Recommended Action

Contact CNA or Target driver support team for assistance.

FCOE-1032

Message

We are in WARM RECOVERING state...

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that high availability (HA) failover or switch reboot may be in progress.

Recommended Action

Wait until the chassis has fully recovered before you perform any operations.

FCOE-1033

Message

FIP v1 FLOGI received on interface <interface info> [WWN <device WWN>] but VF_port <FCoE VF_Port number> has pending logins[Current devices <Current devices>, Pending devices <Pending devices>].

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that a device is trying to log in to a port that already has a device logged in.

FCOE-1034**Message**

Frame [type 0x<Frame type>] received on PFC disabled priority <priority> on interface <interface info> from device <string displaying WWN/MAC> <device WWN/MAC>

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that a frame is received on the specified priority, for which priority-based flow control (PFC) or FCoE is disabled.

Recommended Action

Check FCoE priority on the device or the FSB through which the device is logged in (if applicable) and make sure it matches with the FCoE priority on the switch. In case the FCoE priority on the switch needs to be changed, use `fcoe --config -priority`

FCOE-1037**Message**

Loggingroup dropped for switch WWN: <switch WWN>, due to name conflict while merging.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that same login group name exists for two different switches that have different organizationally unique identifiers (OUIs), but the last three bytes are same.

Recommended Action

Create the login group for the switch World Wide Name (WWN) with another name that will not lead to a name conflict.

FCOE-1038**Message**

logingroup#<login group number> (<login group name>) created.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the specified login group is added to the switch login group table.

FCOE-1039**Message**

Login rejected for interface <interface info> [Device MAC <Device MAC>, WWN <Device WWN>]. No VF_Ports available for login.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that there are no VF ports available for login, hence the logins are rejected.

Recommended Action

If the max number of VF_Ports for the chassis has not reached, create more FCoE VF_Ports using `fcoe --config - endoes`.

FCOE-1040**Message**

Login group name changed from <old login group name> to <new login group name>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the login group has been renamed.

FCOE-1041**Message**

Transaction aborted.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the ongoing FCoE login configuration transaction is aborted.

FCOE-1042**Message**

FCoE login configuration transaction saved fabric-wide.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the FCoE login configuration transaction is saved fabric-wide.

FCOE-1043**Message**

FCoE login configuration management disabled.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the FCoE login configuration management is disabled.

FCOE-1044**Message**

FCoE login configuration management enabled.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the FCoE login configuration management is enabled.

FCPD Messages

Fibre Channel Protocol daemon error messages.

FCPD-1001**Message**

Probing failed on <error string>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that a Fibre Channel Protocol (FCP) switch probed devices on a loop port, and probing failed on the L_Port, arbitrated loop physical address (AL_PA), or the F_Port. For ALPA, the valid range is 0x00 through 0xFF. The *error* variable can be either of the following:

- L_Port *port_number* ALPA *alpha_number*
- F_Port *port_number*

This could happen due to some firmware issue with the device controller on the specified port.

Recommended Action

Contact the device vendor for any firmware-related issues. Also, consider upgrading the device firmware.

FCPD-1002**Message**

port <port number>, bad R_CTL for fcp probing: 0x<R_CTL value>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the response frame received on the specified port for an inquiry request contains an invalid value in the routing control field. This could happen due to some firmware issue with the device controller on the specified port.

Recommended Action

Contact the device vendor for any firmware-related issues. Also, consider upgrading the device firmware.

FCPD-1003**Message**

Probing failed on <error string> which is possibly a private device which is not supported in this port type.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that device probing has failed because private devices will not respond to the switch port login (PLOGI) during probing.

Recommended Action

The Brocade 4100, 4900, 5000, 7500, and AP 7600 do not support private loop devices. Refer to the switch vendor for a list of other port types that support private devices for inclusion into the fabric.

FCPH Messages

Fibre Channel Physical Layer module error messages.

FCPH-1001

Message

<function>: <failed function call> failed, out of memory condition.

Message Type

FFDC | LOG

Message Severity

CRITICAL

Probable Cause

Indicates that the switch is low on memory and failed to allocate new memory for a Fibre Channel driver instance.

The *function* value can only be `fc_create`. This function creates a Fibre Channel driver instance.

The *failed function call* can only be `kmalloc_wrapper`, which has failed. This function call is for kernel memory allocation.

Recommended Action

A non-bladed switch will automatically reboot. For a bladed switch, the active CP blade will automatically fail over and the standby CP will become the active CP.

FCPH-1002

Message

Port <Port Number> has been disabled since switch requires authentication when device authentication policy is set to ON.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates a device that does not support authentication has tried to log in to the switch when the device authentication policy is in ON status on the switch.

Recommended Action

Enable the authentication on the device or set the device authentication status to PASSIVE/OFF on the switch if it is not mandatory. Use the `authUtil` command to change the device authentication policy.

FCPH-1003

Message

Logging out new port <Port Number> with same Port WWN [<Port WWN>] as old port <Port Number>[pid:<Device PID>] due to duplicate Port WWN detection policy.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the specified new port has the same Port World Wide Name (PWWN) as the old port.

FCPH-1004

Message

Logging out new NPIV port <Port Number> with same Port WWN [<Port WWN>] as old port <Port Number>[pid:<Port PID>] due to duplicate Port WWN detection policy.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the specified N_Port ID virtualization (NPIV) port has the same Port World Wide Name (PWWN) as the old port.

FCPH-1005

Message

FDISC exch=0x<ExchangeID> sid=0x<SourceID> did=0x<DestinationID> on port <Port> rejected; temporary mem alloc error. Please bounce port of affected device.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that in busy login conditions, the buffer used for quick memory allocations (known as *atomic malloc*) can be quickly depleted and not replenished before the next allocation occurs.

Recommended Action

Reset the specified port using the `portDisable` and `portEnable` commands.

FCPH-1006**Message**

Core blade ICL port <Port Number> not permitted to come online as its connected to device.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that F_ports were connected to the Core blades.

Recommended Action

Do not attempt to connect devices to the Core blades.

FCPH-1007**Message**

IU is freed. fc(<fc instance>), pt:<port>, frm:<frames_left>, s_id:0x<seq_id>, s_xid:0x<seq_xid>, s_state:0x<seq_state>, s_flags:0x<seq_flags>, s_lst_cnt:0x<seq_last_count>, s_cls:0x<seq_class>, x_pid:<x_x_xid>, x_seq_xid:<x_seq_xid>, x_seq_state:0x<x_seq_state>.

Message Type

FFDC | LOG

Message Severity

WARNING

Probable Cause

Indicates that the sequence memory is already freed.

Recommended Action

If the message persists, execute the `supportSave` command.

FCPH-1008

Message

Indicates that an exchange does not exist while handling an Abort Sequence frame. fc(<fc instance>), pt:<port>, iu_refcnt:<iu_refcnt> sid:0x<sid> did:0x<did> two_abts:<two abts>.

Message Type

FFDC | LOG

Message Severity

WARNING

Probable Cause

Indicates that an exchange does not exist while handling an Abort Sequence frame.

Recommended Action

If the message persists, execute the `supportSave` command.

FCPH-1009

Message

Sequence incomplete and dropped - fc=<fc>, seqid=<Sequence_ID> seq_frames=<Num_Frames_in_Sequence> seq_iu=0x<First_IU_In_Sequence> iu_seq_id=<IU_Sequence_ID> xid=0x<Exchange_ID> sid=0x<Source_ID> did=0x<Destination_ID>

Message Type

LOG

Message Severity

WARNING

Probable Cause

A new sequence is received before a previous sequence is complete. This is likely caused by dropped frames.

Recommended Action

Monitor links for dropped frames due to congestion (class 3 timeouts) and work with device vendor to alleviate the congestion.

FCPH-1010

Message

Logging out old port <Port Number> with same Port WWN [<Port WWN>] as new port <Port Number> due to duplicate Port WWN detection policy.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the specified new port has the same Port World Wide Name (PWWN) as the old port.

FCPH-1011**Message**

Logging out old NPIV port <Port Number>[pid:<Device PID>] with same Port WWN [<Port WWN>] as new port <Port Number> due to duplicate Port WWN detection policy.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the specified new port has the same Port World Wide Name (PWWN) as the old N_Port ID virtualization (NPIV) port.

FCPH-1012**Message**

Logging out old port <Port Number> with same Port WWN [<Port WWN>] as new NPIV port <Port Number> due to duplicate Port WWN detection policy.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the specified N_Port ID virtualization (NPIV) new port has the same Port World Wide Name (PWWN) as the old port.

FCPH-1013

Message

Logging out old NPIV port <Port Number>[pid:<Device PID>] with same Port WWN [<Port WWN>] as new NPIV port <Port Number> due to duplicate Port WWN detection policy.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the specified N_Port ID virtualization (NPIV) new port has the same Port World Wide Name (PWWN) as the old NPIV port.

FCPH-1014

Message

FC Protocol Error: <Protocol_Error> - fc(<fc_instance>) port=<Port_Number> iu=0x<IU_pointer>
nfr=<Num_Frames_in_Sequence> tp=0x<FC_Type> fctl=0x<Frame_Control> seqid=<IU_Sequence_ID>
seqc=<IU_Sequence_Count> xid=0x<IU_Exchange_ID> oxrxid=0x<Originator_Exchange_ID_Responder_Exchange_ID>
sid=0x<Source_ID> did=0x<Destination_ID>

Message Type

LOG

Message Severity

WARNING

Probable Cause

A frame has been received that does not follow the FC Standard Protocol.

Recommended Action

Contact the end device vendor to investigate the condition.

FCR Messages

Fibre Channel router-related traffic and activity on the fabric or back-end fabric.

FCR-1001

Message

FC router proxy device in edge created at port <port number>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that a proxy device at a port in the edge fabric has been imported at the specified port.

FCR-1002

Message

FC router proxy device in edge deleted at port <port number>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that a proxy device at a port in the edge fabric has been deleted at the specified port.

FCR-1003

Message

FC router physical DEVICES newly exported at port <port number>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that one or more physical devices have been newly exported through the specified port.

FCR-1004

Message

FC router physical devices offline at port <port number>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that one or more physical devices connected to the specified port have gone offline.

Recommended Action

Verify that the devices were intended to be taken offline. If not, verify that the devices are functioning properly. Verify that all small form-factor pluggables (SFPs) are seated correctly. Check for faulty cables, deteriorated SFPs, or dirty connections. Replace the cables and the SFPs if necessary.

FCR-1005

Message

FC router LSAN zone device removed at port <port number>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that a device is removed from the logical storage area network (LSAN) zone in the edge fabric.

FCR-1006

Message

FC router LSAN zone device added at port <port number>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that a device is added to a logical storage area network (LSAN) zone in the edge fabric.

FCR-1007**Message**

FC router LSAN zone deleted at port <port number>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that a logical storage area network (LSAN) zone attached to the specified port was deleted in the edge fabric.

FCR-1008**Message**

FC router LSAN zone created at port <port number>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that a logical storage area network (LSAN) zone was created at the specified port in the edge fabric.

FCR-1009**Message**

FC router LSAN zone enabled at port <port number>: <enabled name>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that a logical storage area network (LSAN) zone was enabled in the edge fabric attached to the specified port. The enabled LSAN zone configuration is listed.

FCR-1010**Message**

FC router LSAN zone disabled at port <port number>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that a logical storage area network (LSAN) zone is disabled in the edge fabric attached to the specified port.

FCR-1011**Message**

Remote LSAN zone updated in domain <domain ID>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that a logical storage area network (LSAN) zone update was received from another domain.

FCR-1012**Message**

FC Router fabric build completed on port <port number>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the Fibre Channel router has completed a fabric build at the specified port.

FCR-1013**Message**

Phantom FSPF database exchange completed on port <port number>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the specified EX_Port has completed the fabric shortest path first (FSFP) database exchange.

FCR-1015**Message**

New EX_Port added on port <port number> in domain <domain ID>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that an EX_Port was created on the specified port in the specified domain.

FCR-1016**Message**

FCR fabric no longer reachable at port id <port number> (0x<port number (hex)>) fabric ID <fabric ID>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that a fabric is no longer accessible through the backbone fabric. This may be caused by a link or switch failure.

FCR-1018**Message**

FC router proxy device entries exhausted on port <port number>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the number of proxy devices is greater than allowed by the port resource.

Recommended Action

Remove excess logical storage area network (LSAN) zones or devices until the number of proxy devices exported is within the range allowed by the port resource. Use the `fcResourceShow` command to view resources including LSAN zone resources, LSAN device resources, and proxy device port resources. Use the `fcProxyDevshow` command to view how many proxy devices are created in the fabric with the port resource problem. LSAN zones are removed using standard zoning commands such as `zoneShow`, `zoneRemove`, `zoneDelete`, `cfgDelete`, and `cfgDisable` in the edge fabric. Proxy devices can be removed by zoning operations or by bringing physical devices offline (for example, disabling the port that a device is attached to, and then disconnecting the cable or disabling the device).

FCR-1019**Message**

EX_Port entries exhausted at port <port number>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the number of EX_Port entries being created is greater than allowed by the port resource.

Recommended Action

Disable EX_Ports until the number of ports is within the range allowed by the port resource. The EX_Port limit is displayed using the `fcRouteShow` command. Use the `portDisable` command to disable EX_Ports.

FCR-1020**Message**

Local LSAN zone entries for FC router exhausted; max limit: <LSAN zone limit>; dropped zone: <Zone name>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the number of LSAN zones created within a MetaSAN exceeds the local LSAN zone database limitations.

Recommended Action

Remove excess LSAN zones so that the number of LSAN zones created is within the range of the local database limitations. To do that, perform the following steps:

1. Use the `portDdisable` command to disable all the EX_Ports that received this error message.
2. Use the `portDdisable` command to disable all the other EX_Ports on that FCR connected to the same edge fabrics to which the EX_Ports disabled in step 1 are connected.
3. Use zoning commands on the edge fabrics, to reduce the LSAN zone entries on the edge fabrics.
4. Use the `portEnable` command on each EX_Port, one at a time, and verify that this error is not reported again.

FCR-1021**Message**

Local LSAN device entries exhausted while updating LSAN zone <zone name> device entries.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the number of devices created through logical storage area network (LSAN) zones within the MetaSAN exceeds the local LSAN zone database limitations.

Recommended Action

Remove excess device entries within LSAN zones so that the number of devices is within the range of the local zone database limitations.

FCR-1022**Message**

Local proxy device slot entries exhausted.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that resources to persistently store the proxy device slot to the remote world wide name (WWN) have been consumed.

Recommended Action

Remove the proxy device slots by using the `fcProxyConfig` command or limit proxy devices by removing logical storage area network (LSAN) zone entries.

FCR-1023**Message**

Local phantom port WWN entries exhausted.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the number of port World Wide Names (WWNs) detected to be in use exceeds the local port WWN resources.

Recommended Action

Limit the number of port WWNs required by limiting the remote edge fabric connectivity (which limits the number of translate domains). You can also limit the number of proxy devices for a translate domain (which limits the number of translate domain ports required) by limiting the devices specified in logical storage area network (LSAN) zones.

FCR-1024

Message

Local LSAN zone <zone name> device entries for edge LSAN exhausted; max entries: <Max LSAN zone entries>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the number of devices in a logical storage area network (LSAN) defined in the edge fabric is greater than allowed by the local LSAN zone database limitations.

Recommended Action

Remove excess device entries from this LSAN zone until the number of devices is within the range of the local LSAN zone database limitations.

FCR-1025

Message

Local phantom node WWN entries exhausted.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the number of node World Wide Names (WWNs) detected to be in use exceeds the local node WWN resources.

Recommended Action

Reduce the number of node WWNs required by limiting the remote edge fabric connectivity (which limits the number of translate domains).

FCR-1026

Message

In slot <slot number>, Node WWN roll over.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the node World Wide Name (WWN) pool has rolled over in the specified slot, and WWN entries not detected to be in use are reused as needed.

Recommended Action

It is unlikely that WWN conflicts will occur as a result of pool rollover unless the switch is deployed in a very large MetaSAN environment with a large number of logical storage area network (LSAN) devices and fabrics, or there are highly dynamic changes to EX_Port connectivity. WWN conflicts might cause unpredictable behavior in management applications. To avoid WWN conflicts, all EX_Ports attached to fabrics with highly dynamic changes to EX_Port connectivity should be disabled and then re-enabled.

FCR-1027**Message**

In slot <slot number>, Port WWN roll over.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the port World Wide Name (WWN) pool has rolled over in the specified slot, and WWN entries not detected to be in use are reused as needed.

Recommended Action

It is unlikely that WWN conflicts will occur as a result of pool rollover unless the switch is deployed in a very large MetaSAN environment with a large number of logical storage area network (LSAN) devices and fabrics, or there are highly dynamic changes to EX_Port connectivity. WWN conflicts might cause unpredictable behavior in management applications. To avoid WWN conflicts, all EX_Ports attached to fabrics with highly dynamic changes to EX_Port connectivity should be disabled and then re-enabled.

FCR-1028**Message**

In slot <slot number>, node WWN pool 95 percent allocated.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the node World Wide Name (WWN) pool is close to rollover in the specified slot, and that the WWN entries not detected to be in use will be reused as needed.

Recommended Action

It is unlikely that WWN conflicts will occur as a result of pool rollover unless the switch is deployed in a very large MetaSAN environment with a large number of logical storage area network (LSAN) devices and fabrics, or there are highly dynamic changes to EX_Port connectivity. WWN conflicts might cause unpredictable behavior in management applications. To avoid WWN conflicts, all EX_Ports attached to fabrics with highly dynamic changes to EX_Port connectivity should be disabled and then re-enabled.

FCR-1029**Message**

In slot <slot number>, Port WWN pool 95 percent allocated.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the port World Wide Name (WWN) pool has rolled over in the specified slot, and WWN entries not detected to be in use are reused as needed.

Recommended Action

It is unlikely that WWN conflicts will occur as a result of pool rollover unless the switch is deployed in a very large MetaSAN environment with a large number of logical storage area network (LSAN) devices and fabrics, or there are highly dynamic changes to EX_Port connectivity. WWN conflicts might cause unpredictable behavior in management applications. To avoid WWN conflicts, all EX_Ports attached to fabrics with highly dynamic changes to EX_Port connectivity should be disabled and then re-enabled.

FCR-1030**Message**

Physical device <device WWN> came online at fabric <fabric ID>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the physical device World Wide Name (WWN) came online in the specified fabric.

FCR-1031**Message**

Physical device <device WWN> went offline in fabric <fabric ID>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the physical device World Wide Name (WWN) went offline in the specified fabric.

FCR-1032**Message**

Edge fabric enabled security on port <port number> in fabric <fabric ID>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that Secure mode was turned on in the edge fabric.

FCR-1033**Message**

Edge fabric disabled security on port <port number> in fabric <fabric ID>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that Secure mode was turned off in the edge fabric.

FCR-1034**Message**

LSAN zone added in backbone fabric.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that a new logical storage area network (LSAN) zone was added to the backbone fabric.

FCR-1035**Message**

LSAN zone device <device WWN> added in the backbone fabric.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that a new device to a logical storage area network (LSAN) zone was added to the backbone fabric.

FCR-1036**Message**

LSAN zone <zone name> enabled in the backbone fabric.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the specified logical storage area network (LSAN) zone was enabled in the backbone fabric. The enabled LSAN zone configuration is listed.

FCR-1037**Message**

LSAN zone disabled in the backbone fabric.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that a logical storage area network (LSAN) zone is disabled in the backbone fabric.

FCR-1038**Message**

Total zone entries exceeded local fabric limits by <overflow> entries, in zone: <zone name>, zone limit: <LSAN zone limit>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the number of cfg, zone, or alias entries created in a local fabric is greater than the local switch's zone database limitations.

Recommended Action

Remove excess cfg, zone, or alias entries so that the number of logical storage area network (LSAN) zones created is within the range of the local database limitations.

FCR-1039

Message

Local LSAN zone <zone name> device entries for backbone LSAN exhausted.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the number of devices in the specified logical storage area network (LSAN) defined in the backbone fabric is greater than allowed by the local LSAN zone database limitations.

Recommended Action

Remove excess device entries from this LSAN zone until the number of devices is within the range of the local LSAN zone database limitations.

FCR-1040

Message

Proxy device deleted in the backbone fabric.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that a proxy device created in the backbone fabric was deleted.

FCR-1041

Message

LSAN zone device removed in the backbone fabric.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that a logical storage area network (LSAN) zone device within the backbone fabric was removed.

FCR-1042**Message**

LSAN zone removed in the backbone fabric.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that a logical storage area network (LSAN) zone within the backbone fabric was removed.

FCR-1043**Message**

Proxy device created in the backbone fabric.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that a proxy device was created in the backbone fabric.

FCR-1048**Message**

On EX port (<port number>) setting port <credit type> credits failed.

Message Type

LOG | FFDC

Message Severity

ERROR

Probable Cause

Indicates that the indicated credit type was not set. Setting port credits failed.

Recommended Action

Send the First Failure Data Capture (FFDC) log to the support.

FCR-1049**Message**

EX_Port (<port number>) received an ELP command that is not supported.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates an incoming exchange link parameter (ELP) command that is not supported.

Recommended Action

Use the `portEnable` and `portDisable` to enable or disable the port.

If the problem persists, contact your switch service provider.

FCR-1053**Message**

Port <port number> was disabled, <disable reason>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the specified port was disabled because of a mismatched configuration parameter.

Recommended Action

Use the specified disable reason to identify a possible configuration parameter mismatch between the EX_Port and the switch at the other end of the link.

FCR-1054**Message**

Port <port number> received ILS <command> of incorrect size (<actual payload size>); valid ILS size is <expected payload size>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that an internal link service (ILS) IU of invalid size was received from the switch on the other end of the link.

Recommended Action

Check the error message log on the other switch using the `errShow` command for additional messages.

Check for a faulty cable or deteriorated small form-factor pluggable (SFP). Replace the cable or the SFP if necessary.

Run the `portLogDumpPort` command on both the receiving and transmitting ports.

Run the `fabStatsShow` command on the transmitting switch.

If the message persists, collect switch information using the `supportSave` command, and contact your switch service provider.

FCR-1055**Message**

Switch with domain ID <domain ID> does not support backbone to edge imports.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that a switch that does not support backbone-to-edge routing was detected in the backbone. Edge-to-edge routing will work, but backbone-to-edge routing may fail.

Recommended Action

No action is required if backbone-to-edge routing is not required. Otherwise, replace the switch with one that supports backbone-to-edge routing.

FCR-1056**Message**

Switch <switch WWN> with front domain ID <domain ID> does not support backbone to edge imports.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that a switch that does not support backbone-to-edge routing is running in the MetaSAN.

Recommended Action

No action is required if backbone-to-edge routing is not needed. Otherwise, replace the switch with one that supports backbone-to-edge routing.

FCR-1057**Message**

EX_Port(<port number>) incompatible long distance parameters on link.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the port, which is configured in long distance mode, has incompatible long distance parameters.

Recommended Action

Check the port configuration on both sides of the link using the `portCfgShow` command.

Investigate the other switch for more details. Run the `errShow` command on the other switch to view the error log for additional messages.

FCR-1058

Message

Port <port number> isolated due to mismatched configuration parameter; <segmentation reason>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the specified port was isolated after segmentation caused by mismatched configuration parameters or by a domain ID assigned by the principal switch that did not match the insistent domain ID of this port.

Recommended Action

Check the switches on both ends of the link for a possible mismatch in switch or port configuration parameters such as Operating Mode, E_D_TOV, R_A_TOV, Domain ID Offset, and so on.

Run the `portCfgExport` command to modify the appropriate parameters on the local switch.

Run the appropriate configuration command to modify the switch or port parameters on the remote switch.

FCR-1059

Message

EX_Port <port number> was disabled due to an authentication failure.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the authentication, which uses the Diffie Hellman - Challenge Handshake Authentication Protocol (DH-CHAP), failed on the EX_Port.

Recommended Action

Verify that the shared secrets on both sides of the link match.

Disable and enable the ports by using the `portDisable` and the `portEnable` commands to restart authentication.

FCR-1060

Message

EX_Port(<port number>) has an incompatible configuration setting.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that virtual channel (VC) Link Init is enabled on the local switch and the remote switch is negotiating in R_RDY mode. The fabric might not form properly.

Recommended Action

Check the configuration on the local switch using the `portCfgShow` command to verify that the VC Link Init is disabled, if the remote switch is configured in R_RDY mode or only capable of R_RDY mode.

- VC_RDY mode: Virtual channel flow control mode. This is a proprietary protocol.
- R_RDY mode: Receiver-ready flow control mode. This is the Fibre Channel standard protocol, that uses R_RDY primitive for flow control.

FCR-1061

Message

Backbone fabric created on port <port number>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that a backbone fabric was built on the specified port.

FCR-1062

Message

Port <port number> disabled, system only supports <maximum ports> EX_Ports.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the maximum number of supported EX_Ports was exceeded. To enable the specified port, disable any other operational port and then re-enable the port.

FCR-1063**Message**

Fabric <fabric ID> for switch with domain ID: <domain ID> mismatch with local fabric ID <local fabric ID>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the fabric ID of the switch does not match the local switch.

Recommended Action

Run the `switchShow` command to display the fabric ID. Change the fabric ID to match on both ends by modifying either the local or remote host using the `fcrConfigure` command.

FCR-1064**Message**

Fabric ID of backbone FC-Routers mismatch or overlap with <overlapping fabric principle wwn>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that either a backbone fabric split and both are connected to a common edge fabric, or the fabric ID of two backbone fabrics connected to an edge fabric are the same.

Recommended Action

If the backbone fabric split, merge the fabrics.

If two (or more) backbone fabrics have the same IDs, make the fabric IDs unique using the `fcConfigure` command.

FCR-1065**Message**

Fabric on port <port number> was assigned two different fabric IDs<fabric message>

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that another port on the switch is connected to the same edge fabric with a different fabric ID assignment.

Recommended Action

Change the port fabric ID to the same value as the other ports connected to the edge fabric using the `portCfgExport` command.

FCR-1066**Message**

Fabric on port <port number> has the same fabric ID as in another fabric switch <Conflict switch wwn>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that either the fabric split, or there is another fabric (possibly the backbone) that has the same fabric ID as the fabric connected to the specified port.

Recommended Action

If the fabric split, merge the fabrics and manually re-enable the port.

If there is another fabric with the same ID, change the fabric ID for the port using the `portCfgExport` command.

FCR-1067

Message

Zone configurations, total LSAN zones and aliases, exceeded on port <port number> by <overflow> entries; max entries: <LSAN zone limit>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the total number of zone configurations created in connected fabric exceeds the maximum number supported by the Fibre Channel.

The limit includes both active and configured information that is part of the zoning database in the edge fabric. Non-LSAN zones are not counted in the limit.

Recommended Action

Limit the logical storage area network (LSAN) zoning-related zone configuration in the edge fabric connected to this port.

FCR-1068

Message

The FC Routing service is disabled.

Message Type

AUDIT | LOG

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the FC Routing service is disabled. This is caused by issuing the `fosconfig --disable fcr, configDefault`, or the `configDownload` command with the `fcrState` set to 2 (disabled). Note that the FC Routing service is disabled by the factory.

FCR-1069

Message

The FC Routing service is enabled.

Message Type

AUDIT | LOG

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the FC Routing service is enabled. This is caused by the `fosconfig --enable fcr` or the `configDownload` command with the `fcrState` set to 1 (enabled). Note that the FC Routing service is disabled by the factory.

FCR-1070

Message

The FC Routing configuration is set to default.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the FC Routing configuration is set to the default by the user. This removes all prior FC Routing configurations.

FCR-1071

Message

Port <port number> is changed from non FCR port to FCR port.

Message Type

AUDIT | LOG

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the port became an EX_Port.

FCR-1072**Message**

Port <port number> is changed from FCR port to non FCR port.

Message Type

AUDIT | LOG

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the port is no longer an EX_Port.

FCR-1073**Message**

Switch with domain ID <domain ID> in fabric <fabric ID> has lower limit of LSAN Zones supported.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that an older version switch in the backbone or edge that supports a different limit of logical storage area network (LSAN) zones was detected.

Recommended Action

Use the `fcResourceShow` command on all Fibre Channel Routers in the Meta-SAN to find lowest supported LSAN zone limits. Ensure the total number of LSAN zones in the Meta-SAN are within the lowest supported limit of LSAN zones.

FCR-1074**Message**

HA sync lost as remote CP supports only <LSAN Count> LSAN Zones.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the remote control processor (CP) has older firmware, which supports a lower number of logical storage area network (LSAN) zones. This is causing the loss of high availability (HA) sync.

Recommended Action

Keep the number of LSAN zones to the lower limit of the two CPs or upgrade the remote CP.

FCR-1075**Message**

Zone Name configuration is larger than <Zone Name Limit> characters in the edge fabric connected to port <port number>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the zone name configuration size created in the connected fabric exceeds the maximum supported by the FC Router. This size is equal to the total number of characters used by all the zone names in the edge fabric zoning database.

The limit includes both LSAN and non-LSAN zone names defined in the zoning name database of the edge fabric.

Recommended Action

Limit the zone configuration size in the edge fabric connected to this port by either reducing the number of zones or changing the zone names to smaller names.

FCR-1076

Message

Port <port number> disabled, system only supports <maximum fds> front domains.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the maximum number of supported front domains was exceeded. To enable the specified port, disable any other operational front domain and then re-enable the port.

Recommended Action

Make sure to remain within the maximum number of supported front domains.

FCR-1077

Message

Port <port number> rejected fabric binding request/check from the M-Model switch; <Fabric ID>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that an M-Model edge switch attempted to either activate or check the fabric binding. This port will be disabled if this event occurred during a check of fabric binding and not during failure to activate fabric binding. The error is caused when the binding list details configured on the M-Model switch do not match with the currently configured front port domain ID and WWN of the EX_Port on which this operation was attempted.

Recommended Action

Ensure that the M-Model switch has the same currently configured details such as the front port domain ID and WWN of the EX_Port on which this operation was attempted.

FCR-1078

Message

LSAN name <LSAN name> is too long. It is dropped.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates the length of the logical storage area network (LSAN) name exceeds the limit of 64 characters.

Recommended Action

Change the name and reactivate the zone database.

FCR-1079**Message**

Domain <Domain> has conflict matrix database with local domain.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates the specified domain has a different matrix database from the local domain.

Recommended Action

Change the matrix database.

FCR-1080**Message**

The pause response timer for domain <Domain> expired.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that during the Coordinated HotCode protocol, a switch in the fabric has not responded to the pause message which prevented the protocol from completing. Any data traffic disruption observed during the firmware download may have been the result of the rejected pause message.

FCR-1081**Message**

The pause message is rejected by the domain <Domain>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that during the Coordinated HotCode protocol, a switch in the fabric has rejected the pause message which prevented the protocol from completing. Any data traffic disruption observed during the firmware download may have been the result of the rejected pause message.

FCR-1082**Message**

The pause retry count is exhausted for the domain <Domain>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that during the Coordinated HotCode protocol, a switch in the fabric did not accept the pause message which prevented the protocol from completing. Any data traffic disruption observed during the firmware download may have been the result of this issue.

FCR-1083**Message**

The resume message is rejected by the domain <Domain>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that during the Coordinated HotCode protocol, a switch in the fabric has rejected the pause message which prevented the protocol from completing. Any data traffic disruption observed during the firmware download may have been the result of the rejected resume message.

FCR-1084**Message**

The resume retry count is exhausted for the domain <Domain>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that during the Coordinated HotCode protocol, a switch in the fabric did not accept the resume message which prevented the protocol from completing. Any data traffic disruption observed during the firmware download may have been the result of this issue.

FCR-1085**Message**

HA sync lost as remote CP does not support FCR based matrix.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the remote control processor (CP) has older firmware, which does not support the FCR-based matrix while the local CP has the feature enabled. This is causing the loss of the high availability (HA) synchronization.

Recommended Action

Disable the FCR-based matrix or upgrade the remote CP.

FCR-1086**Message**

HA sync lost as remote CP does not support 8Gb/s-capable FC based EX_Ports.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the remote control processor (CP) has older firmware, which does not support 8Gb/s-capable FC based EX_Port. This is causing the loss of the high availability (HA) synchronization.

Recommended Action

Disable 8Gb/s-capable FC based EX_Ports or upgrade the remote CP.

FCR-1087**Message**

ExPort <ExPort > connects to fabric <fabric > with capability to use XISL domain <Domain >.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the EX_Port connects to the logical fabric containing a domain that has the capability to use extended ISL (XISL).

Recommended Action

Disable "Allow to use XISL" mode of the domain by using the `configure` command.

FCR-1088

Message

LSAN <Enforce/Speed> tag <Tag Name> added.

Message Type

AUDIT | LOG

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the user has added a LSAN tag.

FCR-1089

Message

LSAN <Enforce/Speed> tag <Tag Name> removed.

Message Type

AUDIT | LOG

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the user has removed a LSAN tag.

FCR-1091

Message

Backbone Fabric ID changed to <Tag>.

Message Type

AUDIT | LOG

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the backbone fabric ID has been changed.

FCR-1092**Message**

FCR ELS trap entries exhausted.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the FCR ELS trap entries are exhausted.

Recommended Action

Execute the `supportSave` command and contact your switch service provider.

FCR-1093**Message**

<Message> <Master or Slave> interopmode conflicts with <Master or Edge fabric>. Disabling the port.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the EX_Port (master or slave in case of a trunk) is disabled due to interop mode conflict with either trunk master or edge fabric.

Recommended Action

Configure the master or slave EX_Port with the trunk master or edge fabric interop mode.

FCR-1094**Message**

No Integrated Routing license present. EX-Port <ExPort> will not perform device sharing with other Brocade Native mode fabric(s).

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that an EX_Port has been configured in Brocade Native mode. Device sharing will not occur with other Brocade Native mode fabrics because the Integrated Routing license is not installed.

Recommended Action

Install Integrated Routing license if device sharing is needed with other Brocade Native mode fabrics.

FCR-1095**Message**

The EX-Port <ExPort> is configured in '<ExPortMode>' mode which is no longer supported, hence will be disabled.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that an EX_Port has been configured in 'McData/Open/NOS' mode. During HA failover, the EX_Port will be disabled.

Recommended Action

Remove the 'McData/Open/NOS' interop modes in all EX_Ports

FCR-1096

Message

Failed to allocate <data type> for <operation phase>: port <port number>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the authentication process failed because the system is low on memory.

Data type is the payload or structure that failed to get memory.

Operation phase specifies which operation of a particular authentication phase failed.

Recommended Action

Usually this problem is transient. The authentication may fail.

Reinitialize authentication using the `portDisable` and `portEnable` commands or the `switchDisable` and `switchEnable` commands.

If the message persists, run the `supportFtp` command (as needed) to set up automatic FTP transfers; then run the `supportSave` command and contact your switch service provider.

FCR-1097

Message

Failed to get <data type> for <message phase> message: port <port number>, retval <error code>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the authentication process failed to get a particular authentication value at certain phase.

Data type is the payload or structure that failed to get memory.

Recommended Action

Usually this problem is transient. The authentication may fail.

Reinitialize authentication using the `portDisable` and `portEnable` commands or the `switchDisable` and `switchEnable` commands.

If the message persists, run the `supportFtp` command (as needed) to set up automatic FTP transfers; then run the `supportSave` command and contact your switch service provider.

FCR-1098

Message

Invalid message code for <message phase> message: port <port number>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates the receiving payload does not have valid message code for a particular authentication phase.

Recommended Action

Usually this problem is transient. The authentication may fail.

Reinitialize authentication using the `portDisable` and `portEnable` commands or the `switchDisable` and `switchEnable` commands.

If the message persists, run the `supportFtp` command (as needed) to set up automatic FTP transfers; then run the `supportSave` command and contact your switch service provider.

FCR-1099

Message

HA sync lost as remote CP does not support Inter Chassis Link EX_Ports.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the remote control processor (CP) has older firmware that does not support inter-chassis link (ICL) EX_Ports. This is causing loss of the high availability (HA) synchronization.

Recommended Action

Disable EX_Ports on ICL links or upgrade the firmware on remote CP to v7.2.0 or later.

FCR-1100**Message**

16G EX_Port ICL topology for fabric <Fabric ID> is unbalanced.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the current configuration of the EX_Port inter-chassis link (ICL) paths are unbalanced.

Recommended Action

Investigate the current EX_Port ICL configuration to ensure that all recommendations for cabling are satisfied. Once cabling recommendations are satisfied, FCR-1101 message will be generated confirming ICL paths are balanced.

FCR-1101**Message**

16G EX_Port ICL topology for fabric <Fabric ID> is balanced.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the existing EX_Port inter-chassis link (ICL) configuration that was resulting in an unbalanced topology for the corresponding fabric has been corrected.

FCR-1102**Message**

ICL EX_Port <Port Numbers> need to be present in base switch to make a recommended topology.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that some of the ICL ports in a quad small form-factor pluggable (QSFP) are not present in the base switch. Ideally, all ports in the QSFP group should be present in the base switch.

Recommended Action

Move the specified ICL EX_Ports of the QSFP group into the base switch using the `lscfg --config` command.

FCR-1103**Message**

EX_Port <Port Number> ELS PLOGI from did <DID> to sid <SID> wwn <device wwn> NOT ZONED

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that FCR has received an ELS request for unzoned devices

Recommended Action

Send the First Failure Data Capture (FFDC) log to the support.

FCR-1104**Message**

In Edge fabric <Fabric-id> EX-Port <EX-Port>, domain-id <old_did> changes to <new_did>

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that Phantom domain-id got changed in edge fabric

FCR-1105**Message**

FIPS mode is enabled. SHA-1 hash type is not recommended in edge fabric <edge_fabric> connected to EX-Port <port number>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates the received authentication payload from edge fabric contains SHA-1 hash type.

Recommended Action

SHA-1 is not a recommended setting when FIPS is enabled in edge fabric.

FCR-1106**Message**

HA sync lost as remote CP does not support 4K proxy devices on EX_Ports.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the active control processor (CP) has more than 2000 proxies downloaded per EX_Port but the remote CP does not support the same.

Recommended Action

Remote CP needs to be upgraded to v7.4.0 or later firmware version to support the same.

FCR-1107

Message

EICL License is not present and the port <Port Number> will be disabled.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the Enterprise inter-chassis link (EICL) license is absent and the maximum number of directly connected chassis allowed is three.

Recommended Action

Install EICL license.

FCR-1108

Message

EICL License limit is exceeded and the port <Port Number> will be disabled.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the Enterprise inter-chassis link (EICL) license is present and the number of directly connected chassis has exceeded the maximum allowable limit of nine.

Recommended Action

Disable unwanted directly connected ICL links.

FCR-1109

Message

Either domain <Domain> in BB fabric has PRE 7.4 build or EX-Port with RFID is disabled, which will restrict the Location embedded zone feature to work as expected. Dropped LSAN <ZoneName>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that some of the switches in the backbone fabric have pre v7.4 build.

Recommended Action

Upgrade all switches in the backbone fabric to 7.4 or above version.

FCR-1110**Message**

EX_Port Integrated Routing Port on Demand License limit <limit> is exceeded and the port <Port Number> will be disabled.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the user exceeded the number of licensed EX_port limit.

Recommended Action

Disable unwanted port to enable this port or get Integrated Routing Port on Demand (PoD) license to get more links.

FCR-1111**Message**

License not Installed for Integrated Routing and the port <Port Number> will be disabled.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the license not installed to enable EX_port.

Recommended Action

Install Licence for Integrated Routing.

FCR-1112**Message**

EX-Port is not supported when it is connected to the Analytics Monitoring Platform (AMP). Disabling port <Port Number>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that Fibre Channel Routing (FCR) feature is not supported with Analytics Monitoring Platform.

Recommended Action

Not a supported configuration when EX-Port is connected to Brocade Analytics Monitoring Platform.

FCR-1113**Message**

HA sync lost as remote CP supports only <Device Count> devices.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the remote control processor (CP) has older firmware, which supports a lower number of devices. This is causing the loss of high availability (HA) sync.

Recommended Action

Keep the number of devices to the lower limit of the two CPs or upgrade the remote CP.

FCR-1114

Message

FCR router port <port number> cost changed to <cost>.

Message Type

AUDIT | LOG

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that router port cost has been changed.

FCR-1115

Message

FID <FID>: The QSFP connection topology on core chip is not recommended

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the current QSFP connection topology is not recommended.

Recommended Action

Use the `switchShow`, `islShow`, and `lsdbShow` commands to identify the QSFP connectivity to ensure that all recommendations for cabling is satisfied.

FCR-1116

Message

FID <FID>: The existing QSFP connections causing core-edge-core routing have been corrected

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the current QSFP connection that was resulting in unbalanced topology has been corrected.

FCR-1117**Message**

Switch internal lookup got failed, fcr may lose the EX_Port data

Message Type

LOG

Message Severity

ERROR

Probable Cause

Logical fabric lookup would have got failed

Recommended Action

Reboot the switch or disable/enable all the EX_port configuration

FCR-1118**Message**

No Integrated Routing license present. EX-Port will not perform device sharing with other Brocade Native mode fabric(s).

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that an EX_Port has been configured in Brocade Native mode. Device sharing will not occur with other Brocade Native mode fabrics because the Integrated Routing license is not installed.

Recommended Action

Install Integrated Routing license if device sharing is needed with other Brocade Native mode fabrics.

FCR-1119

Message

The EX-Port <PORT> is set to Fabric ID <FID>

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the edge fabric id has been changed.

FCR-1120

Message

The EX-Port <PORT> is set to Front Domain ID <DOMID>

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the Front domain id has been changed.

FCR-1121

Message

Alias <ALIASNAME> is set for FID <FID>

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the FID alias has been configured.

FCR-1122**Message**

Alias is deleted for FID <FID>

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the FID alias has been deleted.

FCR-1123**Message**

Max LSAN count set to <LSANCOUNT>

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the max lsan count is changed.

FCR-1124

Message

Shortest IFL mode <SIFLMODE>

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the shortest IFL mode is changed.

FCR-1125

Message

Negotiate fabric port parameter configuration is in disabled mode, EX-Port <port number> may get isolated/disabled.

Message Type

AUDIT | LOG

Message Class

CFG

Message Severity

WARNING

Probable Cause

Indicates that the EX-Port fabric auto negotiate configuration have mismatch, This parameter needs to be enabled for successful port bringup.

FCR-1126

Message

EX-Port are not allowed to come online at 4G speed, EX-Port <port number> may get isolated/disabled.

Message Type

AUDIT | LOG

Message Class

CFG

Message Severity

WARNING

Probable Cause

EX-Port are not allowed to come online at 4G speed in FOS9.1.0.

FICN Messages

FICN error messages.

FICN-1007

Message

DevDiskEgr:FICON Selective Reset:Path=0x<VEPortNumber HostDomain HostPort DeviceDomain><DevicePort LPAR CUADDR DeviceAddr> State=0x<Current Emulation State> stat_array=0x<the Last 4 Status values that were received from the device>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates a Selective Reset from the channel was received as either a normal part of path recovery or the starting sequence in an error case.

Recommended Action

If there was a job failure associated with this event, contact your vendor's customer support.

FICN-1008

Message

DevDiskEgr:FICON Purge Path received Path=0x<VEPortNumber HostDomain HostPort DeviceDomcontactain><DevicePort LPAR CUADDR DeviceAddr>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates a FICON Purge Path was received from the channel as a part of path recovery.

Recommended Action

If there was a job failure associated with this event, contact your vendor's customer support for assistance.

FICN-1010**Message**

DevDiskEgr:Device level exception flag found for Path=0x<VEPortNumber HostDomain HostPort DeviceDomain><DevicePort LPAR CUADDR DeviceAddr>: Oxid=0x<The OXID that was reported in the Device Level Exception Frame>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates a Device Level Exception frame was received from the FICON channel.

Recommended Action

If there was a job or I/O failure associated with this event, contact your vendor's customer support for assistance.

FICN-1011**Message**

DevDiskIng:XRC Incorrect RRS SeqNum Rcvd Path=0x<VEPortNumber HostDomain HostPort DeviceDomain><DevicePort LPAR CUADDR DeviceAddr> Expected=0x<The RRS Sequence number that was expected from the device> Received=0x<The RRS Sequence number that was actually received from the device> Oxid=0x<The data frame's OXID>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates the Control unit or device presented a Read Record Set Sequence number different from the SDM's expected sequence number.

Recommended Action

If there was an XRC volume or session suspended associated with this event, contact your vendor's customer support for assistance.

FICN-1012**Message**

DevDiskIng:Device level exception found for Path=0x<VEPortNumber HostDomain HostPort DeviceDomain><DevicePort LPAR CUADDR DeviceAddr>: Oxid=0x<The OXID that was reported in the Device Level Exception Frame>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates a Device Level Exception frame received from the FICON direct attached storage device (DASD) Control Unit.

Recommended Action

If there was a job or I/O failure associated with this event, contact your vendor's customer support for assistance.

FICN-1013**Message**

DevDiskIng:Status=0x<Status that was received from the DASD device in an odd state> received in odd state=0x<The current emulation state> from Path=0x<VEPortNumber HostDomain HostPort DeviceDomain><DevicePort LPAR CUADDR DeviceAddr> sent LBY.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that when the device sent the status in an incorrect state, the emulation processing rejected the status with an LBY frame.

Recommended Action

If there was a job or I/O failure associated with this event, contact your vendor's customer support for assistance.

FICN-1014**Message**

DevEgr:Device level exception flag found for Path=0x<VEPortNumber HostDomain HostPort DeviceDomain><DevicePort LPAR CUADDR DeviceAddr>: Oxid=0x<The OXID used to deliver the non-AS Device Level Exception>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates a frame was received that indicated a device level exception.

Recommended Action

If there was an I/O failure associated with this event, contact your vendor's customer support for assistance.

FICN-1015**Message**

DevEgr:cuPath=0x<VEPortNumber HostDomain HostPort DeviceDomain>*****:Discarding Invalid LRCd SOF=0x<The invalid Frame's SOF value (SOFiX or SOFnx)> count=<The total number of frames that have been received from the peer with incorrect FICON LRC values>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates a frame was received from the peer emulation processing with an invalid Longitudinal Redundancy Checking (LRC) values. This indicates data corruption between the emulation processing components.

Recommended Action

Contact your vendor's customer support for assistance.

FICN-1016

Message

DevIng:Received Logical Path Removed response:Path=0x<VEPortNumber HostDomain HostPort DeviceDomain><DevicePort LPAR><CUADDR>**.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates the FICON Control Unit sent a Logical Path Removed (LPR) frame to the FICON channel.

FICN-1017

Message

DevIng:Received Logical Path Established response:Path=0x<VEPortNumber HostDomain HostPort DeviceDomain><DevicePort LPAR><CUADDR>**.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates the FICON Control Unit sent an Logical Path Established (LPE) frame to the FICON channel.

FICN-1019

Message

DevTapeEgr:AS Link Level Reject (LRJ) from Chan on Path=0x<VEPortNumber HostDomain HostPort DeviceDomain><DevicePort LPAR CUADDR DeviceAddr> LastCmd=0x<the Last 4 commands issued to the device> LastStatus=0x<the Last 4 status values received from the device>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates the FICON channel indicated in the path issued a Link Level Reject (LRJ) frame for a sequence from the device.

Recommended Action

If there was a job failure associated with this event, contact your vendor's customer support for assistance.

FICN-1020**Message**

DevTapeEgr:FICON Cancel received Path=0x<VEPortNumber HostDomain HostPort DeviceDomain><DevicePort LPAR CUADDR DeviceAddr> state=0x<the current emulation state for the device> tflags=0x<the current emulation tape control flags for the device> sflags=0x<the current emulation status control flags for the device>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates the FICON channel issued a Cancel sequence for a device in emulation.

Recommended Action

If there was an unexpected job failure associated with this event, contact your vendor's customer support for assistance.

FICN-1021**Message**

DevTapeEgr:FICON Tape Cancel:Path=0x<VEPortNumber HostDomain HostPort DeviceDomain><DevicePort LPAR CUADDR DeviceAddr> Elapsed Time=<the current SIO time in seconds for the device>.<the current SIO time in milliseconds for the device> seconds.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates the FICON channel issued a Cancel sequence for a device in emulation.

Recommended Action

If there was an unexpected job failure associated with this event, contact your vendor's customer support for assistance.

FICN-1022

Message

DevTapeEgr:FICON Selective Reset:Path=0x<VEPortNumber HostDomain HostPort DeviceDomain><DevicePort LPAR CUADDR DeviceAddr> State=0x<the current state of the device that received the selective reset> statArray=0x<the last 4 status values received from the device> cmdArray=0x<the last 4 commands that were issued to the device> tflags=0x<the current emulation tape control flags for the device> sflags=0x<the current emulation status control flags for the device>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates the FICON channel issued a Selective Reset for a device that was active in emulation.

Recommended Action

If there was an unexpected job failure associated with this event, contact your vendor's customer support for assistance.

FICN-1023

Message

DevTapeEgr:FICON Selective Reset:Path=0x<VEPortNumber HostDomain HostPort DeviceDomain><DevicePort LPAR CUADDR DeviceAddr> Elapsed Time=<the current SIO time in seconds for the device>.<the current SIO time in milliseconds for the device> seconds.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates the FICON channel issued a Selective Reset sequence for a device.

Recommended Action

If there was an unexpected job failure associated with this event, contact your vendor's customer support for assistance.

FICN-1024

Message

DevTapeEgr:FICON Purge received Path=0x<VEPortNumber HostDomain HostPort DeviceDomain><DevicePort LPAR CUADDR DeviceAddr>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates the FICON channel issued a Purge Path command sequence for a device.

Recommended Action

If there was an unexpected job failure or I/O error associated with this event, contact your vendor's customer support for assistance.

FICN-1025

Message

DevTapeIng:Auto Sense Data received on Path=0x<VEPortNumber HostDomain HostPort DeviceDomain><DevicePort LPAR CUADDR DeviceAddr> Bytes0-0xB=0x<bytes 0-3 of sense data from the device><bytes 4-7 of sense data from the device><bytes 8-0x0b of sense data from the device>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates the FICON Tape Write Pipelining processed sense data from a FICON device.

Recommended Action

If there was an unexpected job failure or I/O error associated with this event, contact your vendor's customer support for assistance.

FICN-1026

Message

DevTapeInq:UnusualStatus:WriteCancelSelr:Generating Final Ending Status Path=0x<VEPortNumber HostDomain HostPort DeviceDomain><DevicePort LPAR CUADDR DeviceAddr>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates the FICON Tape Write Pipelining is completing an emulated Selective Reset sequence.

Recommended Action

If there was an unexpected job failure or I/O error associated with this event, contact your vendor's customer support for assistance.

FICN-1027

Message

DevTapeInq:Device level exception found for Path=0x<VEPortNumber HostDomain HostPort DeviceDomain><DevicePort LPAR CUADDR DeviceAddr>: Oxid=0x<The OXID of the frame that included the Device Level Exception>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates an active emulation device delivered a Device Level Exception frame to the emulation processing.

Recommended Action

If there was an unexpected job failure or I/O error associated with this event, contact your vendor's customer support for assistance.

FICN-1028

Message

HostDiskInq:FICON Cancel received Path=0x<VEPortNumber HostDomain HostPort DeviceDomain><DevicePort LPAR CUADDR DeviceAddr> state=0x<The current emulation state of the device>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates an active emulation device received a cancel operation from the FICON channel.

Recommended Action

If there was an unexpected job failure or I/O error associated with this event, contact your vendor's customer support for assistance.

FICN-1029**Message**

HostDiskIng:FICON Selective Reset:Path=0x<VEPortNumber HostDomain HostPort DeviceDomain><DevicePort LPAR CUADDR DeviceAddr> state=0x<The current emulation state of the device> LastCmds=0x<The last 4 commands received from the channel for this device> LastStatus=0x<The last 4 status values presented to the channel for this device>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates an active disk emulation device received a Selective Reset from the FICON channel.

Recommended Action

If there was an unexpected job failure or I/O error associated with this event, contact your vendor's customer support for assistance.

FICN-1030**Message**

HostDiskIng:FICON Purge received:Path=0x<VEPortNumber HostDomain HostPort DeviceDomain><DevicePort LPAR CUADDR DeviceAddr>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates an active disk emulation device received a FICON Purge Path from the channel.

Recommended Action

If there was an unexpected job failure or I/O error associated with this event, contact your vendor's customer support for assistance.

FICN-1032**Message**

HostDiskIng:XRC Read Channel Extender Capabilities detected on Path: 0x<VEPortNumber HostDomain HostPort DeviceDomain><DevicePort LPAR CUADDR DeviceAddr>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates the eXtended Remote Copy (XRC) System Data mover was restarted to discover the capabilities of the channel extension equipment.

Recommended Action

No action is required. This is a part of the XRC initialization.

FICN-1033**Message**

HostEgr:Logical Path Established on Path=0x<VEPortNumber HostDomain HostPort DeviceDomain><DevicePort LPAR><CUADDR>**.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates the peer-side FICON Control Unit has accepted a logical path establishment command sequence with the FICON channel.

Recommended Action

No action is required. This is a part of the FICON path initialization.

FICN-1034**Message**

HostEgr:Discarding Invalid LRCd Frame on Path=0x<VEPortNumber HostDomain HostPort
DeviceDomain><DevicePort>***** count=<The total number of frames that have been received with an invalid LRC.>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates the channel emulation processing received a frame with an invalid FICON LRC from the peer. This indicates that the channel side noted corruption from the Control Unit- or device-side processing.

Recommended Action

Contact your vendor's customer support for assistance.

FICN-1035**Message**

HostIng:FICON System Reset received on Path=0x<VEPortNumber HostDomain HostPort
DeviceDomain><DevicePort><LPAR><CUADDR>**.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates a locally connected FICON channel issued a System Reset to the specified FICON Control Unit.

Recommended Action

No action is required. This is a part of the FICON path initialization.

FICN-1036

Message

HostIng:FICON RLP Request on Path=0x<VEPortNumber HostDomain HostPort
DeviceDomain><DevicePort><LPAR><CUADDR>**.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates a locally connected FICON channel issued a Remove Logical Path sequence to the specified FICON Control Unit.

Recommended Action

No action is required. This is a part of the FICON path deactivation.

FICN-1037

Message

HostIng:FICON ELP Request on Path=0x<VEPortNumber HostDomain HostPort
DeviceDomain><DevicePort><LPAR><CUADDR>**.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates a locally connected FICON channel issued an Establish Logical Path sequence to the specified FICON Control Unit.

Recommended Action

No action is required. This is a part of the FICON path activation.

FICN-1040

Message

HostTapeEgr:Tape:CmdReject Sense Data Rcvd:Path=0x<VEPortNumber HostDomain HostPort
DeviceDomain><DevicePort LPAR CUADDR DeviceAddr> LastCmds=0x<Last 4 commands received from the channel

for this device> SenseData:Bytes0-0xB=0x<Bytes 0-3 of sense data from the device><Bytes 4-7 of sense data from the device><Bytes 8-0x0b of sense data from the device>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates an active disk emulation device received a FICON Purge Path from the channel.

Recommended Action

If there was an unexpected job failure or I/O error associated with this event, contact your vendor's customer support for assistance.

FICN-1041

Message

HostTapeEgr:AS Link Level Reject (LRJ) from CU Rx Path=0x<VEPortNumber HostDomain HostPort DeviceDomain><DevicePort LPAR CUADDR DeviceAddr> LastCmd=0x<Last 4 commands issued to this device from the channel> LastStatus=0x<Last 4 status values sent to the channel from this device>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that a Link Level Reject (LRJ) received from a device indicates that the Control Unit has lost the logical path to the Logical Partition (LPAR).

Recommended Action

If this was an unexpected event, contact your vendor's customer support for assistance.

FICN-1042

Message

HostTapeIng:FICON Cancel received Path=0x<VEPortNumber HostDomain HostPort DeviceDomain><DevicePort LPAR CUADDR DeviceAddr> state=0x<the current emulation state for this device>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates a job was canceled during a Tape Write Pipelining.

Recommended Action

If this was an unexpected event (cancel is normally an operator event), contact your vendor's customer support for assistance.

FICN-1043**Message**

HostTapeIng::FICON Selective Reset:Path=0x<VEPortNumber HostDomain HostPort DeviceDomain><DevicePort LPAR CUADDR DeviceAddr> state=0x<the current emulation state for this device> LastCmds=0x<the last 4 commands received from the channel for this device> LastStatus=0x<the last 4 status values presented to the channel for this device>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that protocol errors in emulation in the Control Unit or network errors can cause a Selective Reset.

Recommended Action

If this was an unexpected event, contact your vendor's customer support for assistance.

FICN-1044**Message**

HostTapeIng::FICON Selective Reset:Path=0x<VEPortNumber HostDomain HostPort DeviceDomain><DevicePort LPAR CUADDR DeviceAddr> Elapsed Time=<the number of seconds since the last IO started for this device>.<the number of milliseconds since the last IO started for this device> seconds.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that protocol errors in emulation in the Control Unit or network errors can cause a Selective Reset.

Recommended Action

If this was an unexpected event, contact your vendor's customer support for assistance.

FICN-1045**Message**

HostTapeIng:FICON Purge received:Path=0x<VEPortNumber HostDomain HostPort DeviceDomain><DevicePort LPAR CUADDR DeviceAddr>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates a Purge Path was received from the locally connected FICON channel. This is performed during the path recovery.

Recommended Action

If this was an unexpected event, contact your vendor's customer support for assistance.

FICN-1046**Message**

HostTapeIng:LRJ received on Path=0x<VEPortNumber HostDomain HostPort DeviceDomain><DevicePort LPAR CUADDR DeviceAddr> lastCmds=0x<Last 4 commands received from the channel for this device> lastStatus=0x<Last 4 status values presented to the channel for this device> treating as system reset event.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that a Link Level Reject (LRJ) from a FICON channel indicates that the channel no longer has a path established to the Control Unit.

Recommended Action

This is normally an unexpected event; contact your vendor's customer support for assistance.

FICN-1047**Message**

fcFicSetEmulation:Path=0x<VEPortNumber HostDomain HostPort DeviceDomain><DevicePort LPAR CUADDR DeviceAddr> FDCB Not Idle state=0x<Current emulation state of the FICON device> prevState=0x<Previous emulation state of the FICON device> set to state=0x<The new state to which the device is transitioning>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates there is an internal emulation error. This message should not be encountered.

Recommended Action

This is an unexpected event; contact your vendor's customer support for assistance.

FICN-1048**Message**

DevDiskEgr:FICON Cancel received Path=0x<VEPortNumber HostDomain HostPort DeviceDomain><DevicePort LPAR CUADDR DeviceAddr> state=0x<Current emulation state of the FICON device> sflags=0x<The current emulation status flags>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates the operator has canceled a read or write job.

Recommended Action

This is an unexpected event; contact your vendor's customer support for assistance.

FICN-1049**Message**

ProcessingTirData:Lost Logical Path for Path=0x<VEPortNumber HostDomain HostPort DeviceDomain><DevicePort LPAR CUADDR DeviceAddr><CUADDR>** Index=<Current processing index in the TIR data from the locally connected channel or control unit>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates a TIR received from a FICON endpoint indicates that it no longer has an established path to its peer.

Recommended Action

This is an unexpected event; contact your vendor's customer support for assistance.

FICN-1050**Message**

ProcessEgrTirData:Lost Logical Path for Path=0x<VEPortNumber HostDomain HostPort DeviceDomain><DevicePort LPAR CUADDR DeviceAddr><CUADDR>** Index=<Current processing index in the TIR data from the remotely connected channel or control unit>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates a TIR received from a far-side FICON endpoint indicates that it no longer has an established path to its peer.

Recommended Action

This is an unexpected event; contact your vendor's customer support for assistance.

FICN-1051

Message

XRC Session Established: SessID=<SDM Assigned Session ID>, Path=0x<VEPortNumber HostDomain HostPort DeviceDomain><DevicePort LPAR CUADDR DeviceAddr>

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates a PSF command has been received to initiate an eXtended Remote Copy (XRC) session with the extended direct attached storage device (DASD) device.

Recommended Action

No action is required. This is a part of the XRC session establishment.

FICN-1052

Message

XRC Session Terminated: SessID=<SDM Assigned Session ID>, Path=0x<VEPortNumber HostDomain HostPort DeviceDomain><DevicePort LPAR CUADDR DeviceAddr>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates a PSF command has been received to break an eXtended Remote Copy (XRC) session with the extended direct attached storage device (DASD) device.

Recommended Action

If this was an unexpected event, contact your vendor's customer support for assistance.

FICN-1053

Message

XRC Withdraw From Session: SessID=<SDM Assigned Session ID>, Path=0x<VEPortNumber HostDomain HostPort DeviceDomain><DevicePort LPAR CUADDR DeviceAddr>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates a PSF command has been received to withdraw from the eXtended Remote Copy (XRC) session with the extended direct attached storage device (DASD) device.

Recommended Action

If this was an unexpected event, contact your vendor's customer support for assistance.

FICN-1054**Message**

XRC Device Suspended: SessID=<SDM Assigned Session ID>, Path=0x<VEPortNumber HostDomain HostPort DeviceDomain><DevicePort LPAR CUADDR DeviceAddr>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates a PSF command has been received to suspend an eXtended Remote Copy (XRC) session with the extended direct attached storage device (DASD) device.

Recommended Action

If this was an unexpected event, contact your vendor's customer support for assistance.

FICN-1055**Message**

XRC All Devices Suspended: SessID=<SDM Assigned Session ID>, Path=0x<VEPortNumber HostDomain HostPort DeviceDomain><DevicePort LPAR CUADDR DeviceAddr>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates a PSF command has been received to suspend all extended direct attached storage device (DASD) devices from the eXtended Remote Copy (XRC) session.

Recommended Action

If this was an unexpected event, contact your vendor's customer support for assistance.

FICN-1056**Message**

FICON Emulation Error Error Code=<The internal emulation error code value>, Path=0x<VEPortNumber HostDomain HostPort DeviceDomain><DevicePort LPAR CUADDR DeviceAddr> LastStates=0x<The 4 oldest emulation states for this device><The prior emulation state for this device><The current emulation state for this device>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates an internal coding error within emulation processing.

Recommended Action

This is an unexpected event; contact your vendor's customer support for assistance.

FICN-1057**Message**

Error return from frame generation processing for a FICON device: Path=0x<VEPortNumber HostDomain HostPort DeviceDomain><DevicePort LPAR CUADDR DeviceAddr>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates an internal resource shortage caused an error so that an emulation frame could not be created and sent to a device.

Recommended Action

This is an unexpected event; contact your vendor's customer support for assistance.

FICN-1059**Message**

Error return from frame generation for a FICON Image: Path=0x<VEPortNumber HostDomain HostPort DeviceDomain><DevicePort><LPAR>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates an internal resource shortage caused an error so that an emulation frame could not be created and sent to an Logical Partition (LPAR).

Recommended Action

This is an unexpected event; contact your vendor's customer support for assistance.

FICN-1062**Message**

Ingress Abort:Oxid=0x<the OXID of the aborted exchange>:Path=0x<VEPortNumber HostDomain HostPort DeviceDomain><DevicePort LPAR CUADDR DeviceAddr>:LastStates=0x<prior emulation state array><previous emulation state><current emulation state>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates an abort operation has been received from the local FC interface for an active emulation exchange.

Recommended Action

This is an unexpected event; contact your vendor's customer support for assistance.

FICN-1063

Message

Egress Abort:Oxid=0x<the OXID of the aborted exchange>:Path=0x<VEPortNumber HostDomain HostPort DeviceDomain><DevicePort LPAR CUADDR DeviceAddr>:LastStates=0x<prior emulation state array><previous emulation state><current emulation state>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates an abort operation has been received from a peer FC interface for an active emulation exchange.

Recommended Action

This is an unexpected event; contact your vendor's customer support for assistance.

FICN-1067

Message

Ingress Abort:Oxid=0x<the OXID of the aborted exchange>:Abort for CH=0x<VEPortNumber HostDomain HostPort DeviceDomain><DevicePort LPAR>****.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates an abort operation has been received from a local FC interface for an emulation CH exchange.

Recommended Action

If there were associated I/O errors at the same time as this event, contact your vendor's customer support for assistance.

FICN-1068

Message

Ingress Abort:Oxid=0x<the OXID of the aborted exchange>:Abort for CU=0x<VEPortNumber HostDomain HostPort DeviceDomain><DevicePort LPAR><CUADDR>**.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates an abort operation has been received from a local FC interface for an emulation Control Unit exchange.

Recommended Action

If there were associated I/O errors at the same time as this event, contact your vendor's customer support for assistance.

FICN-1070**Message**

DevTapeIngr:Exceptional Status rcvd on Path=0x<VEPortNumber HostDomain HostPort DeviceDomain><DevicePort LPAR CUADDR DeviceAddr> state=0x<current emulation state> status=0x<the exceptional status value>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates the normal end of tape status (0x0D or 0x05) is received from the device or error status (including Unit Check 0x02) is received from an active emulation device.

Recommended Action

The end of tape is a normal event during pipelining and not the unit check. If there are associated I/O error messages with this event, contact your vendor's customer support for assistance.

FICN-1071**Message**

HostTapeIngr:Tape Loaded on Path=0x<VEPortNumber HostDomain HostPort DeviceDomain><DevicePort LPAR CUADDR DeviceAddr>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates the tape I/Os are processed from a locally connected Logical Partition (LPAR), which indicates that a tape is loaded on a device.

FICN-1072**Message**

DevTapeEgr:Tape Loaded on Path=0x<VEPortNumber HostDomain HostPort DeviceDomain><DevicePort LPAR CUADDR DeviceAddr>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates the tape I/Os are processed from a locally connected Logical Partition (LPAR), which indicates that a tape is loaded on a device.

FICN-1073**Message**

HostTapeIngr:Unloaded:Path=0x<VEPortNumber HostDomain HostPort DeviceDomain><DevicePort LPAR CUADDR DeviceAddr>:states=0x<4 prior emulation states><previous emulation state><current emulation state>:cmds=0x<last 4 commands received from the channel for this device>:status=0x<last 4 status values sent to the channel for this device>:flags=0x<tape report bit flags (0x80-Tape Loaded,0x40-WriteEmul,0x20-RdBlkEmul,0x10-RdCpEmul)>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates a Rewind and Unload I/O has been processed from a locally connected Logical Partition (LPAR), which indicates that a tape should be unloaded on a device.

FICN-1074**Message**

HostTapeIngr:WriteReport:Path=0x<VEPortNumber HostDomain HostPort DeviceDomain><DevicePort LPAR CUADDR DeviceAddr>:Emuls=0x<the number of idle state to non-idle state transitions while this tape was loaded>:Cmds=0x<the number of emulated host write commands processed while this tape was loaded>:Chains=0x<the number of emulated

host chains processed while this tape was loaded>:MBytes=<the number of emulated write Kilobytes processed while this tape was loaded>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates a Rewind and Unload I/O has been processed from a locally connected Logical Partition (LPAR) and Tape Write Pipelining was performed on the currently loaded tape.

FICN-1075**Message**

HostTapeIngr:ReadBlkReport:Path=0x<VEPortNumber HostDomain HostPort DeviceDomain><DevicePort LPAR CUADDR DeviceAddr>:Emuls=0x<the number of idle state to non-idle state transitions while this tape was loaded>:Cmds=0x<the number of emulated host read commands processed while this tape was loaded>:Chains=0x<the number of emulated host chains processed while this tape was loaded>:MBytes=<the number of emulated read Kilobytes processed while this tape was loaded>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates a Rewind and Unload I/O has been processed from a locally connected Logical Partition (LPAR) and Read Block pipelining was performed on the currently loaded tape.

FICN-1076**Message**

HostTapeIngr:ReadCpReport:Path=0x<VEPortNumber HostDomain HostPort DeviceDomain><DevicePort LPAR CUADDR DeviceAddr>:Emuls=0x<the number of idle state to non-idle state transitions while this tape was loaded>:Cmds=0x<the number of emulated host read commands processed while this tape was loaded>:Chains=0x<the number of emulated host chains processed while this tape was loaded>:MBytes=<the number of emulated read Kilobytes processed while this tape was loaded>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates a Rewind and Unload I/O has been processed from a locally connected Logical Partition (LPAR) and Read Channel Program pipelining was performed on the currently loaded tape.

FICN-1077**Message**

DevTapeEgr:Unloaded:Path=0x<VEPortNumber HostDomain HostPort DeviceDomain><DevicePort LPAR CUADDR DeviceAddr>:states=0x<4 prior emulation states><previous emulation state><current emulation state>:cmds=0x<last 4 commands received from the channel for this device>:status=0x<last 4 status values received from the channel for this device>:flags=0x<tape report bit flags (0x80-Tape Loaded,0x40-WriteEmul,0x20-RdBlkEmul,0x10-RdCpEmul)>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates a Rewind and Unload I/O has been processed from a remotely connected Logical Partition (LPAR), which indicates that a tape should be unloaded on a device.

FICN-1078**Message**

DevTapeEgr:WriteReport:Path=0x<VEPortNumber HostDomain HostPort DeviceDomain><DevicePort LPAR CUADDR DeviceAddr>:Emuls=0x<the number of idle state to non-idle state transitions while this tape was loaded>:Cmds=0x<the number of emulated host write commands processed while this tape was loaded>:Chains=0x<the number of emulated host chains processed while this tape was loaded>:MBytes=<the number of emulated write Kilobytes processed while this tape was loaded>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates a Rewind and Unload I/O has been processed from a remotely connected Logical Partition (LPAR) and Write Tape Pipelining was performed on the currently loaded tape.

FICN-1079

Message

DevTapeEgr:ReadBlkReport:Path=0x<VEPortNumber HostDomain HostPort DeviceDomain><DevicePort LPAR CUADDR DeviceAddr>:Emuls=0x<the number of idle state to non-idle state transitions while this tape was loaded>:Cmds=0x<the number of emulated host read commands processed while this tape was loaded>:Chains=0x<the number of emulated host chains processed while this tape was loaded>:MBytes=<the number of emulated read Kilobytes processed while this tape was loaded>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates a Rewind and Unload I/O has been processed from a remotely connected Logical Partition (LPAR) and Read Block pipelining was performed on the currently loaded tape.

FICN-1080

Message

DevTapeEgr:ReadCpReport:Path=0x<VEPortNumber HostDomain HostPort DeviceDomain><DevicePort LPAR CUADDR DeviceAddr>:Emuls=0x<the number of idle state to non-idle state transitions while this tape was loaded>:Cmds=0x<the number of emulated host read commands processed while this tape was loaded>:Chains=0x<the number of emulated host chains processed while this tape was loaded>:MBytes=<the number of emulated read Kilobytes processed while this tape was loaded>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates a Rewind and Unload I/O has been processed from a remotely connected Logical Partition (LPAR) and Read Channel Program pipelining was performed on the currently loaded tape.

FICN-1081

Message

DevTapeIng:LRJ received on Path=0x<VEPortNumber HostDomain HostPort DeviceDomain><DevicePort LPAR CUADDR DeviceAddr> lastCmds=0x<Last 4 commands received from the channel for this device> lastStatus=0x<Last 4 status values presented to the channel for this device> treating as system reset event.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates a Link Level Reject (LRJ) from a FICON channel indicates that the channel does not have a path established to the Control Unit.

Recommended Action

This is normally an unexpected event; contact your vendor's customer support for assistance.

FICN-1087**Message**

DevTeraEgr:AS Link Level Reject (LRJ) from Chan on Path=0x<VEPortNumber HostDomain HostPort DeviceDomain><DevicePort LPAR CUADDR DeviceAddr> LastCmd=0x<the Last 4 commands issued to the device> LastStatus=0x<the Last 4 status values received from the device>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates the FICON channel indicated in the path issued an Link Level Reject (LRJ) frame for a sequence from the device.

Recommended Action

If there was a job failure associated with this event, contact your vendor's customer support for assistance.

FICN-1088**Message**

DevTeraEgr:FICON Cancel received Path=0x<VEPortNumber HostDomain HostPort DeviceDomain><DevicePort LPAR CUADDR DeviceAddr> state=0x<the current emulation state for the device> tflags=0x<the current emulation tera control flags for the device> sflags=0x<the current emulation status control flags for the device>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates the FICON channel issued a Cancel sequence for a device in emulation.

Recommended Action

If there was an unexpected job failure associated with this event, contact your vendor's customer support for assistance.

FICN-1089**Message**

DevTeraEgr:FICON Tera Cancel:Path=0x<VEPortNumber HostDomain HostPort DeviceDomain><DevicePort LPAR CUADDR DeviceAddr> Elapsed Time=<the current SIO time in seconds for the device>.<the current SIO time in milliseconds for the device> seconds.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates the FICON channel issued a Cancel sequence for a device in emulation.

Recommended Action

If there was an unexpected job failure associated with this event, contact your vendor's customer support for assistance.

FICN-1090**Message**

DevTeraEgr:FICON Selective Reset:Path=0x<VEPortNumber HostDomain HostPort DeviceDomain><DevicePort LPAR CUADDR DeviceAddr> State=0x<the current state of the device that received the selective reset> statArray=0x<the last 4 status values received from the device> cmdArray=0x<the last 4 commands that were issued to the device> tflags=0x<the current emulation tera control flags for the device> sflags=0x<the current emulation status control flags for the device>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates the FICON channel issued a Selective Reset for a device that was active in emulation.

Recommended Action

If there was an unexpected job failure associated with this event, contact your vendor's customer support for assistance.

FICN-1091**Message**

DevTeraEgr:FICON Selective Reset:Path=0x<VEPortNumber HostDomain HostPort DeviceDomain><DevicePort LPAR CUADDR DeviceAddr> Elapsed Time=<the current SIO time in seconds for the device>.<the current SIO time in milliseconds for the device> seconds.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates the FICON channel issued a Selective Reset sequence for a device.

Recommended Action

If there was an unexpected job failure associated with this event, contact your vendor's customer support for assistance.

FICN-1092**Message**

DevTeraEgr:FICON Purge received Path=0x<VEPortNumber HostDomain HostPort DeviceDomain><DevicePort LPAR CUADDR DeviceAddr>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates the FICON channel issued a Purge Path command sequence for a device.

Recommended Action

If there was an unexpected job failure or I/O error associated with this event, contact your vendor's customer support for assistance.

FICN-1093

Message

DevTeraIng:Auto Sense Data received on Path=0x<VEPortNumber HostDomain HostPort DeviceDomain><DevicePort LPAR CUADDR DeviceAddr> Bytes0-0xB=0x<bytes 0-3 of sense data from the device><bytes 4-7 of sense data from the device><bytes 8-0x0b of sense data from the device>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates the FICON tera write pipelining processed sense data from a FICON device.

Recommended Action

If there was an unexpected job failure or I/O error associated with this event, contact your vendor's customer support for assistance.

FICN-1094

Message

DevTeraIng:UnusualStatus:WriteCancelSelr:Generating Final Ending Status Path=0x<VEPortNumber HostDomain HostPort DeviceDomain><DevicePort LPAR CUADDR DeviceAddr>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates the FICON tera write pipeline is completing an emulated Selective Reset sequence.

Recommended Action

If there was an unexpected job failure or I/O error associated with this event, contact your vendor's customer support for assistance.

FICN-1095

Message

DevTeraIng:Device level exception found for Path=0x<VEPortNumber HostDomain HostPort DeviceDomain><DevicePort LPAR CUADDR DeviceAddr>: Oxid=0x<The OXID of the frame that included the Device Level Exception>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates an active emulation device delivered a Device Level Exception frame to the emulation processing.

Recommended Action

If there was an unexpected job failure or I/O error associated with this event, contact your vendor's customer support for assistance.

FICN-1096

Message

HostTeraEgr:CmdReject Sense Data Rcvd:Path=0x<VEPortNumber HostDomain HostPort DeviceDomain><DevicePort LPAR CUADDR DeviceAddr> LastCmds=0x<Last 4 commands received from the channel for this device>
SenseData:Bytes0-0xB=0x<Bytes 0-3 of sense data from the device><Bytes 4-7 of sense data from the device><Bytes 8-0x0b of sense data from the device>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates an active Teradata emulation sequence received a Command Reject Sense from the device.

Recommended Action

If there was an unexpected job failure or I/O error associated with this event, contact your vendor's customer support for assistance.

FICN-1097

Message

HostTeraEgr:AS Link Level Reject (LRJ) from CU Rx Path=0x<VEPortNumber HostDomain HostPort DeviceDomain><DevicePort LPAR CUADDR DeviceAddr> LastCmd=0x<Last 4 commands issued to this device from the channel> LastStatus=0x<Last 4 status values sent to the channel from this device>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates a Link Level Reject (LRJ) received from a device indicates that the Control Unit has lost the logical path to the Logical Partition (LPAR).

Recommended Action

If this was an unexpected event; contact your vendor's customer support for assistance.

FICN-1098

Message

HostTeraIng:FICON Cancel received Path=0x<VEPortNumber HostDomain HostPort DeviceDomain><DevicePort LPAR CUADDR DeviceAddr> state=0x<the current emulation state for this device>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates a job was canceled during a Write Tape Pipelining.

Recommended Action

If this was an unexpected event (cancel is normally an operator event), contact your vendor's customer support for assistance.

FICN-1099

Message

HostTeralng::FICON Selective Reset:Path=0x<VEPortNumber HostDomain HostPort DeviceDomain><DevicePort LPAR CUADDR DeviceAddr> state=0x<the current emulation state for this device> LastCmds=0x<the last 4 commands received from the channel for this device> LastStatus=0x<the last 4 status values presented to the channel for this device>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the channel recognized a timeout condition and issued a Selective Reset.

Recommended Action

If this was an unexpected event, contact your vendor's customer support for assistance.

FICN-1100

Message

HostTeralng::FICON Selective Reset:Path=0x<VEPortNumber HostDomain HostPort DeviceDomain><DevicePort LPAR CUADDR DeviceAddr> Elapsed Time=<the number of seconds since the last IO started for this device>.<the number of milliseconds since the last IO started for this device> seconds.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that protocol errors in emulation in the Control Unit or network errors can cause Selective Reset.

Recommended Action

If this was an unexpected event, contact your vendor's customer support for assistance.

FICN-1101

Message

HostTeralng:FICON Purge received:Path=0x<VEPortNumber HostDomain HostPort DeviceDomain><DevicePort LPAR CUADDR DeviceAddr>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates a Purge Path was received from the locally connected FICON channel. This is performed during the path recovery.

Recommended Action

If this was an unexpected event, contact your vendor's customer support for assistance.

FICN-1102

Message

HostTeralng:LRJ received on Path=0x<VEPortNumber HostDomain HostPort DeviceDomain><DevicePort LPAR CUADDR DeviceAddr> lastCmds=0x<Last 4 commands received from the channel for this device> lastStatus=0x<Last 4 status values presented to the channel for this device> treating as system reset event.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates a Link Level Reject (LRJ) from a FICON channel indicates that the channel believes that it no longer has a path established to the Control Unit.

Recommended Action

This is normally an unexpected event; contact your vendor's customer support for assistance.

FICN-1103

Message

DevTeraIngr:Exceptional Status rcvd on Path=0x<VEPortNumber HostDomain HostPort DeviceDomain><DevicePort LPAR CUADDR DeviceAddr> state=0x<current emulation state> status=0x<the exceptional status value>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the status (0x0D or 0x05) indicating the device is going down was received from the device or error status (including Unit Check 0x02) is received from an active emulation device.

Recommended Action

The device doing down is a normal event during pipelining and not the unit check. If there are associated I/O error messages with this event, contact your vendor's customer support for assistance.

FICN-1104

Message

DevTeraEgr:Device Ready on Path=0x<VEPortNumber HostDomain HostPort DeviceDomain><DevicePort LPAR CUADDR DeviceAddr>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates the Teradata device has been initialized and is ready for emulation operations.

FICN-1105

Message

DevTeraIngr:LRJ received on Path=0x<VEPortNumber HostDomain HostPort DeviceDomain><DevicePort LPAR CUADDR DeviceAddr> lastCmds=0x<Last 4 commands received from the channel for this device> lastStatus=0x<Last 4 status values presented to the channel for this device> treating as system reset event.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates a Link Level Reject (LRJ) from a FICON channel indicates that the channel does not have a path established to the Control Unit.

Recommended Action

This is normally an unexpected event; contact your vendor's customer support for assistance.

FICN-1106**Message**

DevPrintEgr:AS Link Level Reject (LRJ) from Chan on Path=0x<VEPortNumber HostDomain HostPort DeviceDomain><DevicePort LPAR CUADDR DeviceAddr> LastCmd=0x<the Last 4 commands issued to the device> LastStatus=0x<the Last 4 status values received from the device>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates the FICON channel indicated in the path issued a Link Level Reject (LRJ) frame for a sequence from the device.

Recommended Action

If there was a job failure associated with this event, contact your vendor's customer support for assistance.

FICN-1107**Message**

DevPrintEgr:FICON Cancel received Path=0x<VEPortNumber HostDomain HostPort DeviceDomain><DevicePort LPAR CUADDR DeviceAddr> state=0x<the current emulation state for the device> tflags=0x<the current emulation tera control flags for the device> sflags=0x<the current emulation status control flags for the device>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates the FICON channel issued a Cancel sequence for a device in emulation.

Recommended Action

If there was an unexpected job failure associated with this event, contact your vendor's customer support for assistance.

FICN-1108**Message**

DevPrintEgr:FICON Tera Cancel:Path=0x<VEPortNumber HostDomain HostPort DeviceDomain><DevicePort LPAR CUADDR DeviceAddr> Elapsed Time=<the current SIO time in seconds for the device>.<the current SIO time in milliseconds for the device> seconds.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates the FICON channel issued a Cancel sequence for a device in emulation.

Recommended Action

If there was an unexpected job failure associated with this event, contact your vendor's customer support for assistance.

FICN-1109**Message**

DevPrintEgr:FICON Selective Reset:Path=0x<VEPortNumber HostDomain HostPort DeviceDomain><DevicePort LPAR CUADDR DeviceAddr> State=0x<the current state of the device that received the selective reset> statArray=0x<the last 4 status values received from the device> cmdArray=0x<the last 4 commands that were issued to the device> tflags=0x<the current emulation tera control flags for the device> sflags=0x<the current emulation status control flags for the device>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates the FICON channel issued a Selective Reset for a device that was active in emulation.

Recommended Action

If there was an unexpected job failure associated with this event, contact your vendor's customer support for assistance.

FICN-1110**Message**

DevPrintEgr:FICON Selective Reset:Path=0x<VEPortNumber HostDomain HostPort DeviceDomain><DevicePort LPAR CUADDR DeviceAddr> Elapsed Time=<the current SIO time in seconds for the device>.<the current SIO time in milliseconds for the device> seconds.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates the FICON channel issued a Selective Reset sequence for a device.

Recommended Action

If there was an unexpected job failure associated with this event, contact your vendor's customer support for assistance.

FICN-1111**Message**

DevPrintEgr:FICON Purge received Path=0x<VEPortNumber HostDomain HostPort DeviceDomain><DevicePort LPAR CUADDR DeviceAddr>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates the FICON channel issued a Purge Path command sequence for a device.

Recommended Action

If there was an unexpected job failure or I/O error associated with this event, contact your vendor's customer support for assistance.

FICN-1112

Message

DevPrintIng:Auto Sense Data received on Path=0x<VEPortNumber HostDomain HostPort DeviceDomain><DevicePort LPAR CUADDR DeviceAddr> Bytes0-0xB=0x<bytes 0-3 of sense data from the device><bytes 4-7 of sense data from the device><bytes 8-0x0b of sense data from the device>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates the FICON Printer write pipelining processed sense data from a FICON device.

Recommended Action

If there was an unexpected job failure or I/O error associated with this event, contact your vendor's customer support for assistance.

FICN-1113

Message

DevPrintIng:LRJ received on Path=0x<VEPortNumber HostDomain HostPort DeviceDomain><DevicePort LPAR CUADDR DeviceAddr> lastCmds=0x<Last 4 commands received from the channel for this device> lastStatus=0x<Last 4 status values presented to the channel for this device> treating as system reset event.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates a Link Level Reject (LRJ) from a FICON channel indicates that the channel does not have a path established to the Control Unit.

Recommended Action

This is normally an unexpected event; contact your vendor's customer support for assistance.

FICN-1114

Message

DevPrintIng:Device level exception found for Path=0x<VEPortNumber HostDomain HostPort DeviceDomain><DevicePort LPAR CUADDR DeviceAddr>: Oxid=0x<The OXID of the frame that included the Device Level Exception>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates an active emulation device delivered a Device Level Exception frame to the emulation processing.

Recommended Action

If there was an unexpected job failure or I/O Error associated with this event, contact your vendor's customer support for assistance.

FICN-1115

Message

HostPrintEgr:CmdReject Sense Data Rcvd:Path=0x<VEPortNumber HostDomain HostPort DeviceDomain><DevicePort LPAR CUADDR DeviceAddr> LastCmds=0x<Last 4 commands received from the channel for this device>
SenseData:Bytes0-0xB=0x<Bytes 0-3 of sense data from the device><Bytes 4-7 of sense data from the device><Bytes 8-0x0b of sense data from the device>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates an active Print emulation sequence received Command Reject Sense data from the device.

Recommended Action

If there was an unexpected job failure or I/O error associated with this event, contact your vendor's customer support for assistance.

FICN-1116

Message

HostPrintEgr:AS Link Level Reject (LRJ) from CU Rx Path=0x<VEPortNumber HostDomain HostPort DeviceDomain><DevicePort LPAR CUADDR DeviceAddr> LastCmd=0x<Last 4 commands issued to this device from the channel> LastStatus=0x<Last 4 status values sent to the channel from this device>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that a Link Level Reject (LRJ) was received from a device indicating that the Control Unit has lost the logical path to the Logical Partition (LPAR).

Recommended Action

If this was an unexpected event; contact your vendor's customer support for assistance.

FICN-1117

Message

HostPrintIng:FICON Cancel received Path=0x<VEPortNumber HostDomain HostPort DeviceDomain><DevicePort LPAR CUADDR DeviceAddr> state=0x<the current emulation state for this device>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates a job was canceled during Print write pipelining.

Recommended Action

If this was an unexpected event (cancel is normally an operator event), contact your vendor's customer support for assistance.

FICN-1118

Message

HostPrintIng::FICON Selective Reset:Path=0x<VEPortNumber HostDomain HostPort DeviceDomain><DevicePort LPAR CUADDR DeviceAddr> state=0x<the current emulation state for this device> LastCmds=0x<the last 4 commands received from the channel for this device> LastStatus=0x<the last 4 status values presented to the channel for this device>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the channel recognized a timeout condition and issued a Selective Reset.

Recommended Action

If this was an unexpected event, contact your vendor's customer support for assistance.

FICN-1119

Message

HostPrintIng::FICON Selective Reset:Path=0x<VEPortNumber HostDomain HostPort DeviceDomain><DevicePort LPAR CUADDR DeviceAddr> Elapsed Time=<the number of seconds since the last IO started for this device>.<the number of milliseconds since the last IO started for this device> seconds.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the channel recognized a timeout condition and issued a Selective Reset.

Recommended Action

If this was an unexpected event, contact your vendor's customer support for assistance.

FICN-1120

Message

HostPrintIng:FICON Purge received:Path=0x<VEPortNumber HostDomain HostPort DeviceDomain><DevicePort LPAR CUADDR DeviceAddr>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates a Purge Path was received from the locally connected FICON channel. This is performed during FICON path recovery.

Recommended Action

If this was an unexpected event, contact your vendor's customer support for assistance.

FICN-1121

Message

HostPrintIng:LRJ received on Path=0x<VEPortNumber HostDomain HostPort DeviceDomain><DevicePort LPAR CUADDR DeviceAddr> lastCmds=0x<Last 4 commands received from the channel for this device> lastStatus=0x<Last 4 status values presented to the channel for this device> treating as system reset event.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates than a Link Level Reject (LRJ) received from a FICON channel indicates that the channel no longer has a path established to the Control Unit.

Recommended Action

This is normally an unexpected event; contact your vendor's customer support for assistance.

FICN-1122

Message

DevPrintIng:UnusualStatus:WriteCancelSelr:Generating Final Ending Status Path=0x<VEPortNumber HostDomain HostPort DeviceDomain><DevicePort LPAR CUADDR DeviceAddr>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates the FICON Print write pipeline sequence has received unit check status.

Recommended Action

If there was an unexpected job failure or I/O error associated with this event, contact your vendor's customer support for assistance.

FICN-1123

Message

Path=<VEPortNumber HostDomain HostPort DeviceDomain DevicePort><printf>***** is operating with Fibre Channel Endpoint Security feature on an emulation enabled VE Port.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that FICON encrypted flows were encountered on the emulation-enabled VE_Port.

Recommended Action

FICON Emulation features do not support Fibre Channel Endpoint Security flows. Either disable FICON Features on the tunnel or disable Fibre Channel Endpoint Security on the associated CHPID (Channel Path).

FICN-2064

Message

Ingress Abort:Oxid=0x<the OXID of the aborted exchange>:Unknown Path on VEPort=<VEPortNumber> from SID=0x<Source Domain><Source Port> to DID=0x<Destination Domain><Destination Port>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates an abort operation has been received from a local FC interface for an exchange.

Recommended Action

If there were associated I/O errors at the same time as this event, contact your vendor's customer support for assistance.

FICN-2065**Message**

Egress Abort:Oxid=0x<the OXID of the aborted exchange>:Unknown Path on VEPort=<VEPortNumber> from SID=0x<Source Domain ><Source Port> to DID=0x<Destination Domain><Destination Port>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates an abort operation has been received from a peer FC interface for an exchange.

Recommended Action

If there were associated I/O errors at the same time as this event, contact your vendor's customer support for assistance.

FICN-2066**Message**

MemAllocFailed for VEport=<VEPortNumber> could not create required structure.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates an internal resource limit has been encountered so that additional control block memory could not be allocated.

Recommended Action

This is an unexpected event; either the maximum number of emulation devices are already in use or there is an internal memory leak. Contact your vendor's customer support for assistance.

FICN-2082**Message**

EmulEls:CSWR_RSCN received on VEPort=<VEPortNumber> Domain=0x<Host/Device Side Domain> Port=0x<Host/Device Side Port>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates an attached port which had a FICON emulated path established has logged out from the switch.

Recommended Action

This may be an unexpected event; contact your vendor's customer support for assistance.

FICN-2087**Message**

FICON connected 3900 printer discovered Path=0x<VEPortNumber HostDomain HostPort DeviceDomain><DevicePort LPAR CUADDR DeviceAddr>-invalid compression mode.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that FICON Printer emulation is enabled, but cannot be performed for this device because the compression mode on the tunnel is not set to None or Aggressive.

Recommended Action

If you desire FICON Printer emulation for this device, modify the tunnel compression mode to None (mode 0) or Aggressive (mode 3).

FICU Messages

FICON-CUP daemon error messages.

FICU-1001

Message

<error message>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that one of the configuration management functions have failed. The *key* variable is a component of the Fabric OS configuration database and is for support use only. The *error* variable is an internal error number.

Recommended Action

Execute the `haFailover` command on the switch if it has redundant control processors (CPs) or reboot the switch. Execute the `switchStatusShow` command to check if the flash memory is full. If the flash memory is full, execute the `supportSave` command to clear the core files.

FICU-1002

Message

<function name>: Failed to get Switch Node Descriptor data from Management Server for Domain=<domain> rc=<error>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the fibre connectivity control unit port (FICON-CUP) daemon failed to get the Switch Node Descriptor data from the management server because of a Fabric OS problem. The *domain* variable displays the domain ID of the switch or logical switch for which the Node Descriptor was requested. The *error* variable is an internal error number.

Recommended Action

If this is a bladed switch, execute the `haFailover` command. If the problem persists, or if this is a non-bladed switch, download a new firmware version using the `firmwareDownload` command.

FICU-1003**Message**

<function name>: <message> FICON-CUP License Not Installed: (<error>).

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the fibre connectivity control unit port (FICON-CUP) license is not installed on the switch.

Recommended Action

Execute the `licenseShow` command to check the installed licenses on the switch. The switch cannot be managed using FICON-CUP commands until the FICON-CUP license is installed. Contact your switch supplier for a FICON-CUP license. Execute the `licenseAdd` command to add the license to your switch.

FICU-1004**Message**

<function name>: Failed to set FICON Management Server (FMS) mode: conflicting PID Format:<pid_format>, FMS Mode:<mode>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that a process ID (PID) format conflict was encountered. The core PID format is required for fibre connectivity control unit port (FICON-CUP).

The *pid_format* variable displays the PID format currently running on the fabric, and is one of the following:

- 0 - VC-encoded PID format
- 1 - Core PID format
- 2 - Extended-edge PID format

The *mode* variable displays whether FICON Management Server (FMS) mode is enabled, and is one of the following: 0 means FMS mode is enabled and 1 means FMS mode is disabled.

Recommended Action

To enable FMS mode, the core PID format must be used in the fabric. Change the PID format to core PID using the `configure` command and re-enable FMS Mode using the `ficonCupSet` command. Refer to the *Fabric OS Administrator's Guide* for information on core PID mode.

FICU-1005

Message

Failed to initialize <module>, rc = <error>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that initialization of a module within the fibre connectivity control unit port (FICON-CUP) daemon failed.

Recommended Action

Download a new firmware version using the `firmwareDownload` command.

FICU-1006

Message

Control Device Allegiance Reset: (Logical Path: 0x<PID>:0x<channel image ID>).

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the path with the specified Port Identifier (PID) and channel image ID lost allegiance to a fibre connectivity control unit port (FICON-CUP) device.

Recommended Action

Check if the FICON channel corresponding to the PID in the message is functioning correctly.

FICU-1007

Message

<function name>: Failed to allocate memory while performing <message>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that memory resources are low. This may be a transient problem.

Recommended Action

Check the memory usage on the switch using the `memShow` command.

If the message persists, execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

FICU-1008

Message

FMS mode has been enabled. Port(s):<port number(s)> have been disabled due to port address conflict.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the specified ports were disabled when the FICON Management Server (FMS) mode was enabled. This is due to a port address conflict or the port address being reserved for the CUP management port.

FICU-1009

Message

FMS Mode enable failed due to insufficient frame filtering resources on some ports.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the frame filtering resources required to enable FICON Management Server mode (fmsMode) were not available on some of the ports.

Recommended Action

Execute the `haFailover` command on the switch if it has redundant control processors (CPs) or reboot the switch.

FICU-1010**Message**

FMS mode enable failed due to port(s) with areas 0xFE or 0xFF is(are) connected to device(s).

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the FICON Management Server (FMS) mode was not enabled because ports with areas 0xFE or 0xFF are connected to devices.

Recommended Action

Disable ports with areas 0xFE or 0xFF using the `portDisable` command.

FICU-1011**Message**

FMS mode has been enabled.

Message Type

AUDIT | LOG

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the FICON Management Server mode (fmsMode) has been enabled.

FICU-1012**Message**

FMS mode has been disabled.

Message Type

AUDIT | LOG

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the FICON Management Server mode (fmsMode) has been disabled.

FICU-1013**Message**

Host data file cannot be reset to proper size.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the file system is too full to create the host data file at the proper size.

Recommended Action

Execute the `df` command to check if the flash memory is full. If the flash memory is full, execute the `supportSave` command to clear the core files.

FICU-1017**Message**

FMSMODE enable failed because reserved area is bound to a device.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that one or both of the reserved areas 0xFE and 0xFF is bound to a device.

Recommended Action

Execute the `wwnaddress --show` command to display all devices currently bound to areas. Execute the `wwnaddress --unbind` command to release the reserved area from the device.

FICU-1018**Message**

FMSMODE enable noticed swapped ports.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that some ports are swapped at the time FICON Management Server mode (fmsMode) is enabled.

Recommended Action

Verify the expected FICON port address and port number relationship. For more information, refer to the "FICON and FICON CUP in Virtual Fabrics" section of the *FICON Administrator's Guide*.

FICU-1019**Message**

Switch has been set offline by Logical Path(<Logical Path ID>).

Message Type

AUDIT | LOG

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the FICON Host at the Logical Path shown has disabled the switch.

FICU-1020**Message**

Port Addr (<port mask>) have been Blocked by <source>.

Message Type

AUDIT | LOG

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the port has been blocked.

FICU-1021**Message**

Port Addr (<port mask>) have been Unblocked by <source>.

Message Type

AUDIT | LOG

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates the port has been unblocked.

FICU-1022

Message

Detected FC8-48 and/or FC8-64 that are not manageable when FMS mode is enabled.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates the presence of unmanageable ports such as 48-port blade ports in the virtual fabric-disabled chassis.

FICU-1025

Message

MAPS Evt Notif - <Action taken by FICUD when it received a MAPS Event Notification> - HSC((0x<HSC code associated with the MAPS MSid>),(<HSC text that will appear on the MVS Console>)), RuleN(<MAPS rule name supplied in the MAPS Event Notification>), MSid(<MAPS MSid supplied in the MAPS Event Notification>), Obj(<MAPS Object description from ObjKeyValue from the MAPS Event Notification>, <MAPS Object instance from ObjKeyValue in the MAPS Event Notification>), CondN(<MAPS Condition supplied in the MAPS Event Notification>), MSVal(<MAPS MS Value supplied in the MAPS Event Notification>).

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that Monitoring and Alerting Policy Suite (MAPS) alert has been processed by the control unit port (CUP).

FICU-1026

Message

MAPS Rule Action Notification - <Action (Code) taken by MAPS a rule was triggered> - Action(0x<Action (Descr) taken by MAPS a rule was triggered>, <Severity >), Sev(<Object Identifier (Code)>), Obj(<Object Identifier (Descr)>, <printf>).

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that Monitoring and Alerting Policy Suite (MAPS) has notified FMS CUP that it has taken an action as a result of a rule being triggered.

FICU-1030**Message**

Host Initiated Supportsave (Logical Path: 0x<PID>:0x<Channel Image ID>) failed because Auto-FTP is OFF.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that Auto_FTP is not configured when a Host Initiated Supportsave request was received.

FICU-1031**Message**

Host Initiated Supportsave (Logical Path: 0x<PID>:0x<Channel Image ID>) failed because a Supportsave is already in progress.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that a Supportsave is already in progress when a Host Initiated Supportsave request was received.

FICU-1032**Message**

Host Initiated Supportsave (Logical Path: 0x<PID>:0x<Channel Image ID>) has started to the remote host.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that a Host Initiated Supportsave has started.

FICU-1033**Message**

FMS mode enabled in a non-FICON logical switch. You must convert to a FICON logical switch or FICON devices will fail to attach.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates a configuration error has been detected.

Recommended Action

Convert the logical switch to a FICON logical switch.

FICU-1035**Message**

Error unblocking Port Address (<port mask>) Source (<source>).

Message Type

AUDIT | LOG

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that an error occurred unblocking a port.

FICU-1036**Message**

FOS 9.0.0 is the last release to support the Allow/Prohibit matrix. \ See the FOS 9.0.0 FICON Config Guide.
Src(<source>)

Message Type

LOG

Message Severity

WARNING

Probable Cause

FOS 9.0.0 is the last release to support the Prohibit Dynamic Connectivity Mask (PDCM) used for connectivity management as reflected in the Allow/Prohibit matrix. Effectively, the PDCM feature is deprecated from Fabric OS 9.1.0. Brocade recommends using Fabric OS zoning instead for connectivity management functions. See the FOS 9.0.0 FICON Config Guide for more information.

FICU-1037**Message**

Ignored the Prohibited connections that are detected in the Allow/Prohibit matrix configuration during HA sync <HA Operation> operation.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that an PDCM dump or update operation has PDCM prohibits present in them, and the PDCM prohibits are ignored.

FKLB Messages

Fabric OS I/O kernel library module error messages.

FKLB-1001

Message

exchange <xid> overlapped, pid=<pid>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the FC kernel driver has timed out the exchange while the application is still active. When the FC kernel driver reuses the exchange, the application will overlap. This happens on a timed-out exchange; it automatically recovers after the application times out the exchange.

FLOD Messages

FLOD error messages.

FLOD-1001

Message

Unknown LSR type: port <port number>, type <LSR header type>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the link state record (LSR) type is unknown. The following two LSR header types are the only known types:

- 1 - Unicast
- 3 - Multicast

Recommended Action

No action is required; the record is discarded.

FLOD-1003

Message

Link count exceeded in received LSR, value = <link count number>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the acceptable link count received was exceeded in the link state record (LSR).

Recommended Action

No action is required; the record is discarded.

FLOD-1004**Message**

Excessive LSU length = <LSU length>.

Message Type

LOG | FFDC

Message Severity

ERROR

Probable Cause

Indicates that the link state update (LSU) size exceeds the value the system can support.

Recommended Action

Reduce the number of switches in the fabric or reduce the number of redundant inter-switch links (ISLs) between two switches.

FLOD-1005**Message**

Invalid received domain ID: <domain number>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the received link state record (LSR) contained an invalid domain number.

Recommended Action

No action is required; the LSR is discarded.

FLOD-1006**Message**

Transmitting invalid domain ID: <domain number>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the transmitted link state record (LSR) contained an invalid domain number.

Recommended Action

No action is required; the LSR is discarded.

FLOD-1007**Message**

The LSR for reachable domain <domain number> reached the maximum age and has been removed from the LSDB.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the link state record (LSR) in the local switch's Link State Database (LSDB) for a domain reachable in the fabric hit the maximum LSR age of 3600 seconds. After flooding the aged out record to the other switches, the LSR was removed from the LSDB and the fabric shortest path first (FSPF) calculations were run to update the routes accordingly.

Recommended Action

Check the switch for the reported domain to make sure it did not crash, become unresponsive, or is experiencing frame transmission issues. Next check for any inter-switch link (ISL) ports on the switch reporting the RASLog that may be flapping up and down rapidly resulting in premature LSR aging.

FSPF Messages

Fabric Shortest Path First (FSPF) error messages.

FSPF-1001

Message

Input Port <port number> out of range.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the specified input port number is out of range because it does not exist on the switch.

Recommended Action

No action is required. This is a temporary kernel error that does not affect your system. If the problem persists, execute the `supportSave` command and contact your service provider.

FSPF-1002

Message

Wrong neighbor ID (<domain ID>) in Hello message from port <port number>, expected ID = <domain ID>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the switch has received a wrong domain ID from its neighbor switch in the HELLO message from a specified port. This may happen when a domain ID for a switch has been changed.

FSPF-1003

Message

Remote Domain ID <domain number> out of range, input port = <port number>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the specified remote domain ID is out of range.

Recommended Action

No action is required. The frame is discarded.

FSPF-1005

Message

Wrong Section Id <section number>, should be <section number>, input port = <port number>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that an incorrect section ID was reported from the specified input port. The section ID is part of the fabric shortest path first (FSPF) protocol and is used to identify a set of switches that share an identical topology database.

Recommended Action

This switch does not support a non-zero section ID. Any connected switch from another manufacturer with a section ID other than 0 is incompatible in a fabric of Brocade switches. Disconnect the incompatible switch.

FSPF-1006

Message

FSPF Version <FSFP version> not supported, input port = <port number>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the fabric shortest path first (FSPF) version is not supported on the specified input port.

Recommended Action

Update the FSPF version by running the `firmwareDownload` command. All current versions of the Fabric OS support FSPF version 2.

FSPF-1007**Message**

ICL triangular topology is broken between the neighboring domains: <domain number> and <domain number>. Please fix it ASAP.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the inter-chassis link (ICL) triangular topology is broken and becomes linear. It may cause frame drop or performance slowdown.

Recommended Action

Connect the two domains using ICL or regular inter-switch link (ISL) to form a triangular topology.

FSPF-1008**Message**

ICL triangular topology is formed among the domains: <domain number> (self), <domain number>, and <domain number>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the inter-chassis link (ICL) triangular topology is formed.

FSPF-1009

Message

ICL topology is not recommended on local domain <domain number>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the current inter-chassis link (ICL) topology is not recommended.

Recommended Action

Use the `switchShow`, `islShow`, and `lsdbShow` commands to identify the neighbor domains that violate the ICL connectivity requirement.

FSPF-1010

Message

ICL Topology is valid on local domain <domain number>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the current inter-chassis link (ICL) topology is valid for routing from the local switch.

FSPF-1011

Message

ICL topology is unbalanced.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the current configuration of inter-chassis link (ICL) paths are unbalanced.

Recommended Action

Investigate current ICL configuration to ensure that all recommendations for cabling are satisfied.

FSPF-1012**Message**

All existing ICL topology imbalances have been corrected.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the existing inter-chassis link (ICL) configuration that was resulting in an unbalanced topology has been corrected.

FSPF-1013**Message**

Exceeded maximum number of supported paths (16) to one or more remote domains.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that there are more than 16 (maximum number of paths supported) available shortest cost paths to reach one or more remote domains. Traffic may be impacted or follow unexpected traffic patterns.

Recommended Action

Use the `fabricShow -paths`, `topologyShow`, and `lsDbShow` commands to get additional details about which remote domains are violating the maximum paths limit. Refer to the *Fabric OS Administrator's Guide* for information on the causes and potential impacts.

FSPF-1014

Message

All previously reported maximum path violations have been corrected.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that all existing violations of the maximum paths limit have been corrected.

FSPF-1015

Message

Static link costs are not supported on AE_Ports. Resetting link cost to default for port <port index> from <old link cost value>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that when an analytics E_Port or T_Port comes online and if there is a statically defined linkcost for the port, then the link cost of the port will be cleared and returned to the default value.

FSPF-1016

Message

Port decommissioning request for port <port number> completed successfully. (Neighbor WWN: <printf>)

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the previously issued port decommissioning request has completed successfully.

FSPF-1017**Message**

Fabric topology invalid: remote domain(s) only reachable via path(s) through a non-routing switch.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that one or more domains in the fabric are only reachable via a switch that does not support routing traffic through it.

This can happen, for example, if an AMP switch is in the only path between any two switches in the same fabric.

While the fabric is in this state due to the invalid topology, the fabric is unstable and incomplete. For all switches in the fabric, some new ports are blocked from coming online. Also, some fabric wide configuration operations, such as zone commits, may fail or be blocked. The switch may also report RTWR messages.

This message may be reported during transient situations while the fabric is still forming. If so, then a FSPF-1018 message should be seen once the fabric finished forming and the topology is valid.

Recommended Action

Correct the topology by providing eligible paths that do not pass through the non-routing switch. This may require additional connections or investigation of ISLs that failed to come online.

Alternatively, disable links between the non-routing switch and the domains only accessible via that switch.

FSPF-1018**Message**

All previous remote domain(s) reachability restrictions via non-routed switches cleared.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that any previously detected fabric reachability problems due to non-routed switches have all been cleared.

FSPF-1019

Message

Incomplete LISL topology detected.

Message Type

LOG | FFDC

Message Severity

WARNING

Probable Cause

The LISL full mesh topology failed to form as expected resulting in domains only being reachable via paths that traverse multiple consecutive LISL hops, which is not supported.

Recommended Action

Investigate why the full mesh among all the Logical Switches on the common base fabric has failed to form properly.

This is often caused by one of the Logical ISL links not completing the bring up and either hasn't reach the E-Port state, or is having transmission issues. Check the FSPF `nbrStateShow` for any links that are not in the NB_ST_FULL State and Done Sub-State.

FSPF-1020

Message

All previously reported LISL topology issues have been fixed.

Message Type

LOG

Message Severity

INFO

Probable Cause

Any previously detected and reported LISL topology issues have been fixed.

FSS Messages

Fabric OS state synchronization framework module error messages.

FSS-1001

Message

Component (<component name>) dropping HA data update (<update ID>).

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that an application has dropped a high availability (HA) data update.

Recommended Action

For a dual control processor (CP) system, enable the HA state synchronization using the `haSyncStart` command. For non-bladed systems, restart the switch using the `reboot` command.

If the problem persists, execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

FSS-1002**Message**

Component (<component name>) sending too many concurrent HA data update transactions (<dropped update transaction ID>).

Message Type

LOG

Message Severity

CRITICAL

Probable Cause

Indicates that an application has sent too many concurrent high availability (HA) data updates.

Recommended Action

For a dual CP system, enable the HA state synchronization using the `haSyncStart` command. For non-bladed systems, restart the switch using the `reboot` command.

If the problem persists, execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

FSS-1003**Message**

Component (<component name>) misused the update transaction (<transaction ID>) without marking the transaction beginning.

Message Type

LOG | FFDC

Message Severity

WARNING

Probable Cause

Indicates that the Fabric OS state synchronization (FSS) service has dropped the update because an application did not set the transaction flag correctly.

Recommended Action

For a dual CP system, enable the high availability (HA) state synchronization using the `haSyncStart` command. For non-bladed systems, restart the switch using the `reboot` command.

If the problem persists, execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

FSS-1004

Message

Memory shortage.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the system ran out of memory.

Recommended Action

Execute the `memShow` command to view memory usage in the switch.

For a dual CP system, enable the high availability (HA) state synchronization using the `haSyncStart` command. For non-bladed systems, restart the switch using the `reboot` command.

If the problem persists, execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

FSS-1005

Message

FSS read failure.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the read system call to the Fabric OS state synchronization (FSS) device has failed.

Recommended Action

If the problem persists, execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

FSS-1006**Message**

No FSS message available.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that data is not available on the Fabric OS state synchronization (FSS) device.

Recommended Action

If the problem persists, execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

FSS-1007**Message**

<component name>: Faulty Ethernet connection.

Message Type

LOG

Message Severity

CRITICAL

Probable Cause

Indicates that the Ethernet connection between the active control processor (CP) and the standby CP is not healthy. This error occurs when the standby CP does not respond to a request from the active CP within five seconds. This usually indicates a problem with the internal Ethernet connection and the disruption of the synchronization process.

Recommended Action

Execute the `supportShow` or `supportSave` command to validate the network configuration and then execute the `haSyncStart` command to restore the high availability (HA) synchronization. If the problem persists, contact your switch service provider.

FSS-1008**Message**

FSS Error: <Error Message>.

Message Type

LOG

Message Severity

CRITICAL

Probable Cause

Indicates that a Fabric OS state synchronization (FSS) error has occurred.

Recommended Action

Execute the `supportSave` command and contact your switch service provider.

FSS-1009**Message**

FSS Error: <Error Message>.

Message Type

LOG | FFDC

Message Severity

ERROR

Probable Cause

Indicates that a Fabric OS state synchronization (FSS) error has occurred for the specified component. The error code is displayed in the message.

Recommended Action

Execute the `supportSave` command and contact your switch service provider.

FSS-1010**Message**

FSS Warning: <Warning Message>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that a Fabric OS state synchronization (FSS) error may have occurred.

Recommended Action

Execute the `supportSave` command and contact your switch service provider.

FSS-1011**Message**

FSS Info: <Info Message>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates a Fabric OS state synchronization (FSS) related informational message.

FSSM Messages

Fabric OS State Synchronization Management module error messages.

FSSM-1002**Message**

HA State is in sync.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the high availability (HA) state of the active control processor (CP) is in synchronization with the HA state of the standby CP. If the standby CP is healthy, the failover will be nondisruptive.

FSSM-1003**Message**

HA State out of sync.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the high availability (HA) state of the active control processor (CP) is out of synchronization with the HA state of the standby CP. If the active CP failover occurs when the HA state is out of synchronization, the failover is disruptive.

Recommended Action

If this message was logged as a result of a user-initiated action (such as running the **reboot** command), no action is required.

Otherwise, execute the `haSyncStart` command on the active CP to resynchronize the HA state.

If the HA state does not synchronize, execute the `haDump` command to diagnose the problem.

If the problem persists, execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

FSSM-1004**Message**

Incompatible software version in HA synchronization.

Message Type

LOG

Message Severity

CRITICAL

Probable Cause

Indicates that the active control processor (CP) and the standby CP in a dual CP system are running firmware that is incompatible with each other. If the active CP fails, the failover will be disruptive.

In a switch system, this message is logged when a firmware upgrade or downgrade was invoked. The new firmware version is not compatible with the current running version. This causes a disruptive firmware upgrade or downgrade.

Recommended Action

For a dual CP system, execute the `firmwareDownload` command to load compatible firmware on the standby CP.

FSSM-1005**Message**

Standby CP does not support more than 8 LS.

Message Type

LOG | FFDC

Message Severity

CRITICAL

Probable Cause

Indicates that the active control processor (CP) is configured with more than 8 Logical Switches (LS) and the standby CP is running firmware that does not support more than 8 LS, due to which high availability (HA) is not synchronized between the active CP and the standby CP.

Recommended Action

For a dual CP system, execute `firmwareDownload` command to load compatible firmware that supports more than 8 LS on the standby CP.

FTC Messages

Fabric Traffic Controller module error messages.

FTC-1001**Message**

Received Peer Congestion FPIN [event type: <Event_Type>] from device PID:0x<N_Port_ID>

Message Type

LOG

Message Severity

INFO

Probable Cause

Specified device is reporting a congestion condition.

Recommended Action

Investigate fabric topology for oversubscription potential.

FTC-1002

Message

Received Link Integrity FPIN [event type: <Event_Type>] from device PID:0x<N_Port_ID>

Message Type

LOG

Message Severity

INFO

Probable Cause

Specified device has detected a link integrity issue.

Recommended Action

Diagnose the physical port (e.g., SFP, cabling, etc.).

FV Messages

Flow Vision module error messages.

FV-1001

Message

Flow Vision daemon initialized.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the Flow Vision daemon has successfully initialized.

FV-1002

Message

Flow Vision Config Replay Completed Successfully.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the Flow Vision config replay has successfully completed.

FV-1003

Message

Flow <Flow name> is deactivated. Reason: <Reason for deactivation>

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the specified flow is deactivated automatically by the system.

Recommended Action

Verify the message using the specified reason for deactivation.

No action is required if the message indicated by the specified reason is correct. Otherwise, activate the flow using the `flow --activate` command.

FV-1004

Message

One or more flows are deactivated. Reason: <Reason for deactivation>

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that some of the flows are deactivated automatically by the system.

Recommended Action

Verify the message using the specified reason for deactivation.

No action is required if the message indicated by the specified reason is correct. Otherwise, activate the flow using the `flow --activate` command.

FV-1007**Message**

The FC trace file for flow <flowName> has been processed. File <fileName> created.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the FC Trace capture for the given flow is ready.

Recommended Action

The file can be uploaded using `flowCapture --upload` for offline viewing.

FV-1008**Message**

The total buffer space allocated for pcap files created has reached 90 percent threshold.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that further flow activation may fail.

Recommended Action

Remove the pcap files using `flowCapture --delete file_name` to make space for new pcap files.

FV-1009**Message**

There is a failure in processing FC trace file for flow <flowName>. File creation failed.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates error in processing the pcap file of FC Trace capture for the given flow.

FV-1010**Message**

The FC trace flow <flowName> has been deleted successfully.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates the deletion of FC Trace flow.

FV-1011**Message**

Maximum IT limit for sys_flow_monitor flow has been changed from <oldIT> to <newIT>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates new IT limit that can be monitored for sys_flow_monitor flow.

FV-1012**Message**

Activation of <flow_name> flow has failed as Flow Vision license is not present or has expired.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates flow activation failure.

Recommended Action

Install a valid Flow Vision license to activate the flow.

FV-3000**Message**

Flow <flow_name> is created with features <feature_list>.

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the specified flow has been created.

FV-3001**Message**

Flow <flow_name> is deleted.

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the specified flow has been deleted.

FV-3002

Message

Flow <flow_name> is activated for the feature(s) <feature_list>.

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the specified flow has been activated.

FV-3003

Message

Flow <flow_name> is deactivated for the feature(s) <feature_list>.

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the specified flow has been deactivated.

FV-3004**Message**

Configuration of Flow <flow_name> is changed for the feature(s) <feature_list>.

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that configuration of the specified flow has been changed.

FV-3005**Message**

Flow <flow_name> is reset for the feature(s) <feature_list>.

Message Type

AUDIT | LOG

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the specified flow is being reset.

FV-3006**Message**

Port(s)<range_string><port_number> is(are) being configured as SIM Port. Some of the ports may not be eligible to become SIM Port.

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the specified ports are configured as SIM ports.

FV-3007**Message**

Port(s)<range_string><port_number> being deconfigured as SIM Port. Some of the ports may be already deconfigured as SIM Port.

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the specified ports are deconfigured as SIM ports.

FV-3008**Message**

All ports are being configured as SIM Port. Some of the ports may not be eligible to become SIM Port.

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that all ports are configured as SIM ports.

FV-3009**Message**

All ports being deconfigured as SIM Port. Some of the ports may be already deconfigured as SIM Port.

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that all ports are deconfigured as SIM ports.

FV-3010**Message**

Control configuration for flows has been changed.

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that control configuration has been changed.

FV-3011

Message

Control configuration has been changed for all applicable flows.

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that control configuration has been changed for all applicable flows.

FV-3012

Message

All flows are deactivated for the feature(s) <feature_list>.

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that all flows are deactivated.

FV-3013

Message

All user created flows are deleted.

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that all user created flows are deleted.

FV-3014**Message**

All flows are reset for the feature(s) <feature_list>.

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates all flows are reset for the specified features.

FV-3015**Message**

Aging time of <days> days and <hours> hours is configured for 'sys_mon_analytics' flow.

Message Type

AUDIT | LOG

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that aging time is configured.

FV-3016

Message

IT Reserve Limit <itLimit> and ITL Reserve Limit <itlLimit> are configured for 'sys_mon_analytics' flow.

Message Type

AUDIT | LOG

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that Initiator and Target (IT) and Initiator, Target and LUN (ITL) reserve limits are configured.

FV-3017

Message

Max ITL Per IT Limit <maxItlPerIt> is configured for 'sys_mon_analytics' flow.

Message Type

AUDIT | LOG

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that Maximum Initiator Target LUN (ITL) per Initiator Target (IT) limit is configured.

FV-3018

Message

The IT count limit has reached its maximum <Count> for the chip <Chip> in slot <Slot>. This chip cannot learn new ITs or ITLs.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the Initiator Target (IT) flow count limit has reached its maximum value.

FV-3019**Message**

The ITL count limit has reached its maximum <Count> for the chip <Chip> in slot <Slot>. This chip cannot learn new ITs or ITLs.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the Initiator Target LUN (ITL) flow count limit has reached its maximum value.

FV-3020**Message**

The IT count limit for the switch has reached its maximum value <Count>. This switch cannot learn new ITs or ITLs.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the Initiator Target (IT) flow count limit has reached its maximum value.

FV-3021**Message**

The ITL count limit for the switch has reached its maximum value <Count>. This switch cannot learn new ITs or ITLs.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the Initiator Target LUN (ITL) flow count limit has reached its maximum value.

FV-3022**Message**

Flow count limit for the chassis has reached its Maximum value <Count>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that chassis level flow count limit has reached its Maximum value.

FV-3023**Message**

Configuration has been auto-updated to monitor <Chip> errors for the chip <Slot> in the slot <printf>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that new set of error monitoring has been configured for IO flows at chip level.

FV-3024**Message**

Switch FID has been changed from <oldFid> to <newFid>, \"sys_flow_monitor\" is being reset to delete stale flows.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates flows with old FID are no more valid

FV-3025**Message**

"sys_flow_monitor\" flow was disrupted, may result in 1 minute metric loss on user port(s) \"<User Port>\".

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates flows on the port could have lost some metrics

FV-3026**Message**

Real time pinning flow count limit has reached its Maximum <Count>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that real time collections flow count limit has reached its Maximum value.

FV-3027**Message**

Deactivate/Reset in progress, please retry the operation after some time.

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates previous deactivation/reset is in progress on sys_flow_monitor

FVS Messages

FVS error message.

FVS-1001

Message

Flow Vision Stats daemon initialized.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the Flow Vision Stats daemon has successfully initialized.

GE5 Messages

Golden Eye5 (GE5) module error messages.

GE5-1001

Message

S<slot number>,P<port number>(Bp<blade port number>) user_idx:<User port index> [PID 0x<24 bit FC address>] faulted due to invalid SFP, conflicting speed or laser fault. <error message>

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates a deteriorated small form-factor pluggable (SFP) transceiver, an incompatible SFP transceiver pair, or a faulty cable between the peer ports.

Recommended Action

Verify that compatible SFP transceivers are used on the peer ports, that the SFP transceivers have not deteriorated, and that the Fibre Channel cable is not faulty. Replace the SFP transceivers or the cable if necessary.

GE5-1002**Message**

Port <port number> chip failed due to an internal error.

Message Type

LOG | FFDC

Message Severity

ERROR

Probable Cause

Indicates an internal error. All ports on the blade or switch will be disrupted.

Recommended Action

To recover a bladed system, execute the `slotPowerOff` and `slotPowerOn` commands on the blade. To recover a nonbladed system, execute the `fastBoot` command on the switch.

GE5-1004**Message**

S<slot number>,C<chip index>: Invalid DMA ch pointer, chan:<Channel number>, good_addr:0x<Good address>
bad_addr:0x<Bad address>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates an internal error in the application-specific integrated circuit (ASIC) hardware that may degrade the data traffic.

Recommended Action

Reboot the system at the next customer maintenance window. If the problem persists, replace the blade.

GE5-1006

Message

S<slot number>,C<chip index>: Various non-critical hardware errors were observed: fault1:0x<fault1_cnt>, fault2:0x<fault2_cnt> thresh1:0x<threshold_used>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that some errors were found in the hardware that may or may not impact the data traffic.

Recommended Action

No action is required. Usually these errors are transient.

GE5-1007

Message

S<slot number>,P<port number>(<blade port number>): best effort QoS will be turned off at next port state change as it is not supported under this configuration.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that Quality of Service (QoS) will be turned off automatically at the next port state change because best effort QoS is no longer supported on 8Gb/s platform long-distance ports.

GE5-1008

Message

S<slot number>,P<port number>(<blade port number>): QoS overwrites portcfglongdistance vc_translation_link_init. ARB will be used on the link.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that Quality of Service (QoS) has overwritten the fill word IDLE used on the long-distance links. Arbitrated loop (ARB) will be used on the link.

GE5-1009**Message**

S<slot number>,P<port number>(<blade port number>): portcfglongdistance vc_translation_link_init = 1 overwrites fill word IDLE. ARB will be used on the link.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the `portcfglongdistance vc_translation_link_init 1` command has overwritten the fill word IDLE. Arbitrated loop (ARB) will be used on the link.

GE5-1010**Message**

S<slot number>,C<chip index>: Above normal hardware errors were observed: fault1:0x<fault1_cnt>, fault2:0x<fault2_cnt> thresh2:0x<threshold_used>.

Message Type

LOG

Message Severity

CRITICAL

Probable Cause

Indicates that above-normal errors were observed in the hardware that may or may not impact the data traffic.

Recommended Action

When this error is observed persistently, power-cycle the specified blade using the `slotPowerOff` and `slotPowerOn` commands. If the problem persists, replace the blade.

GE5-1011

Message

Detected a complete loss of credit on internal back-end VC: Slot <slot number>, Port <port number>(<blade port number>) vc_no=<vc number> crd(s)lost=<Credit(s) lost>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that all credits have been lost on the specified virtual channel (VC) and port.

Recommended Action

Turn on back-end credit recovery to reset the link and recover the lost credits. If credit recovery has already been turned on, the link will be reset to recover the credits and no action is required.

GE5-1012

Message

S<slot number>,P<port number>(<blade port number>): Link Timeout on internal port ftx=<frame transmitted> tov=<real timeout value> (><expected timeout value>) vc_no=<vc number> crd(s)lost=<Credit(s) lost> complete_loss:<Complete credit loss>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that one or more credits have been lost on a back-end port and that there has been no traffic on that port for two seconds.

Recommended Action

Turn on back-end credit recovery to reset the link and recover the lost credits. If credit recovery has already been turned on, the link will be reset to recover the credits and no action is required.

GE5-1013

Message

Multi RDY/Frame Loss detected on internal port of Slot <slot number>, Port <port number>(<blade port number>) m_rdy(0x<Multiple Credit(s) Lost>)/m_frame(0x<Multiple Frame(s) Lost>).

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that wait cycles to recover the lost frame or credit have been exceeded on the specified port.

Recommended Action

Turn on back-end credit recovery to reset the link and recover the lost credits. If credit recovery has already been turned on, the link will be reset to recover the credits and no action is required.

GE5-1014

Message

Link Reset on Port S<slot number>,P<port number>(<blade port number>) vc_no=<vc number> crd(s)lost=<Credit(s) lost> <Source of link reset > trigger.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that one or more credits were lost and that the link has been reset.

Recommended Action

When this error is observed persistently on back-end link, power-cycle the specified blade using the `slotPowerOff` and `slotPowerOn` commands. If the problem persists, replace the blade. When this error is observed persistently on a user port, check the physical layer errors on this port and peer port using `portStatsShow` command. If there are some physical layer errors, change the small form-factor pluggable (SFP) transceiver or the cable on the port and peer port to which this port is connected.

GE5-1015

Message

Port re-initialized due to Link Reset failure on internal Port S<slot number>,P<port number>(<blade port number>).

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the specified port has re-initialized due to a link reset failure.

Recommended Action

When this error is observed persistently, power-cycle the specified blade using the `slotPowerOff` and `slotPowerOn` commands. If the problem persists, replace the blade.

GE5-1016

Message

Port is faulted due to port re-initialization failure on internal Port S<slot number>,P<port number>(<blade port number>) with reason <port fault reason>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the specified port failed due to a port re-initialization failure.

Recommended Action

When this error is observed persistently, power-cycle the specified blade using the `slotPowerOff` and `slotPowerOn` commands. If the problem persists, replace the blade.

GE5-1017

Message

Blade in Slot-<slot number> failed due to unavailability of ports in the internal trunk.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the specified blade failed because of the unavailability of the ports in the internal trunk.

Recommended Action

When this error is observed persistently, power-cycle the specified blade using the `slotPowerOff` and `slotPowerOn` commands. If the problem persists, replace the blade.

GE5-1018**Message**

Link reset threshold value exceeded in the link S<slot number>,P<port number>(<blade port number>).

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the specified blade has faulted because the link reset threshold value was exceeded.

Recommended Action

When this error is observed persistently, power-cycle the specified blade using the `slotPowerOff` and `slotPowerOn` commands. If the problem persists, replace the blade.

GE5-1019**Message**

S<slot number>,C<chip index>: HW ASIC Chip TXQ FID parity error threshold reached type = 0x<chip error type>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that an internal error has been observed in the application-specific integrated circuit (ASIC) hardware that may degrade the data traffic.

Recommended Action

Restart the system at the next customer maintenance window.

GE5-1020**Message**

S<slot number>,P<port number>(<blade port number>): Internal CRC with good EOF errors were observed, continuing monitoring. current:0x<last_crc_good_eof_cnt>, last:0x<total_crc_good_eof_cnt> thresh1:0x<threshold_used>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that some CRC errors were detected on a back-end link by the hardware. Typically applications are not affected at this low count.

GE5-1023**Message**

Single RDY/Frame Loss detected and recovered on Slot <slot number>,Port <port number>(<blade port number>) rdy(0x<Credit Lost>)/frame(0x<Frame Lost>).

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that above-normal errors have been observed in the hardware that may or may not impact the data traffic.

Recommended Action

When this error is observed persistently, power-cycle the specified blade using the `slotPowerOff` and `slotPowerOn` commands. If the problem persists, replace the blade.

GE5-1028

Message

Detected excessive Link resets on the port in a second. Slot <slot number>, Port <port number>(<blade port number>).

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the port received excessive link resets from the peer port within 1 second and that exceeded the threshold.

Recommended Action

When this error is observed persistently, change the small form-factor pluggable (SFP) transceiver or the cable on the peer port to which this port is connected.

GE5-1030

Message

S<slot number>,P<port number>(<blade port number>): Internal CRC with good EOF errors exceeded threshold, tuning is required. current:0x<last_crc_good_eof_cnt>, last:0x<total_crc_good_eof_cnt> thresh2:0x<threshold_used>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that some CRC errors have been detected on back-end link by hardware; applications may be affected.

Recommended Action

If a core blade reset or auto tuning or manual tuning does not resolve the issue, replace the blade.

GE5-1031

Message

LOSYNC timeout occurred on Slot <slot number>, Port <port number>(<blade port number>).

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that loss of synchronization has occurred on the BE port and that a link reset was invoked on this port by the blade driver.

GE5-1032**Message**

S<slot number>,P<port number>(<blade port number>): Required buffer unavailable for the port. req_buf:<required buffer> port_buf:<port buffer> unused_buf:<Unused buffer> est_buf:<Estimated buffer>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that free buffers in the chip are not sufficient to bring the port online in fully operational mode. The port may not come online or may operate in a degraded buffer mode.

Recommended Action

If one or more ports that are configured as long distance in the chip are unused, reset these ports to normal distance. If the problem persists, move the affected port to a different blade or chip.

GE5-1033**Message**

S<slot number>,P<port number>(<blade port number>): FEC TTS is only supported on F_Port.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that Forward Error Correction (FEC) TTS is enabled on the specified port. The FEC TTS option is supported only on F_Ports.

Recommended Action

Disable the FEC TTS option using the `portcfgfec --disable -TTS` command.

GE5-1034**Message**

S<slot number>,P<port number>(<blade port number>): FEC is Enabled but FEC is Inactive. Check peer port's FEC configurations.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that Forward Error Correction (FEC) is enabled but is inactive on the specified port.

Recommended Action

Check the local and peer port's FEC configurations using the `portcfgfec --show` command.

GE5-1035**Message**

Credit Recovery disabled on Slot <slot number>, Port <port number>(<blade port number>) because of HW error.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that credit recovery logic has failed.

Recommended Action

Disable and enable the port, and if the error persists, disable credit recovery for the port.

GE5-1036

Message

Buffer sharing unfairness issue on Slot <slot number>, Port <port number>(<blade port number>).

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates buffer sharing unfairness and port starvation.

GE5-1037

Message

S<slot number>,C<chip index>: DAE Error, first error top = 0x<first error top>, intr_cause = 0x<intr cause>, first_err = 0x<first error> first_err_info 0x<first error info>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that a hardware parity error has been detected in the Goldeneye5 DAE block.

Recommended Action

DAE counters may have been corrupted; ignore DAE flow counters in the last polling cycle.

GE5-1038

Message

Slow drain device quarantine (SDDQ) or Restore action is not completed for the sid 0x<Source ID>, did 0x<Destination ID>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the Frame Transformation Block (FTB) entry has not been added.

GE5-1039**Message**

S<slot number>,C<chip index>: Temperature is <current temperature>, maximum threshold is <Maximum operating temperature>. If it exceeds threshold, the unit will be shutdown.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the operating environment conditions are causing the application-specific integrated circuit (ASIC) to overheat.

Recommended Action

Make sure that the area is well ventilated and that the room temperature is within the operational range of your switch. Refer to the hardware reference manual for your switch for the operational temperature range.

GE5-1040**Message**

Multi RDY/Frame Loss detected on Slot <slot number>, Port <port number>(<blade port number>) m_rdy(0x<Multiple Credit(s) Lost>)/m_frame(0x<Multiple Frame(s) Lost>). Link Reset done.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that multiple credits and frames were lost on the specified port and that the link has reset.

GE5-1041

Message

Encryption block error event detected on Slot <slot number>, Port <port number>(<blade port number>), err_count:<error counter>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that encryption block errors have been detected.

Recommended Action

Disable and enable the port, and if the problem persists, replace the blade.

GE5-1042

Message

Port in Slot <slot number>, Port <port number>(<blade port number>) getting faulted because of encryption block error.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the port has faulted because of encryption block errors.

Recommended Action

Disable and enable the port, and if the problem persists, replace the blade.

GE5-1043

Message

Encryption enabled Port S<slot number>,P<port number>(<blade port number>) faulted due to link initialization failure.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that an encryption-configured port failed because of a link initialization failure.

Recommended Action

Disable and enable the port, and if the problem persists, replace the blade.

GE5-1044**Message**

Trunk performance impact on port (<port number>) due to high deskew value. [TRUNK_PERF:<perf> percent, Deskew:<deskew>]

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates a high deskew value on the port.

Recommended Action

Check for physical cable length differences among physical ports of the trunk. If there are cable length differences, fix them with the same cable length link. Otherwise replace the cable if the problem persists.

GE5-1045**Message**

Single parity error detected in ftb statistics memory, slot <slot> index <index>

Message Type

LOG

Message Severity

INFO

Probable Cause

A parity error was detected in FTB statistics memory; a Flow Vision flow monitor may show incorrect statistics.

Recommended Action

Reset the Flow Vision flow monitor flow that is showing abnormal statistics.

GE5-1046**Message**

Multiple parity errors detected in ftb statistics memory, slot <slot> indexes <index> <index> <index> <index>

Message Type

LOG

Message Severity

INFO

Probable Cause

A parity error was detected in FTB statistics memory; a Flow Vision flow monitor may show incorrect statistics.

Recommended Action

Reset the Flow Vision flow monitor flow that is showing abnormal statistics.

GE5-1048**Message**

S<Slot number>,C<Chip Index>: Maximum possible buffers (<Maximum possible buffers>) exceeded; total desired:<Total Number of buffers desired>; port <Port with high desired count> has high desired count:<Desired buffer count on the one port>

Message Type

LOG | FFDC

Message Severity

ERROR

Probable Cause

More buffers have been requested/desired than exist on the ASIC. This will cause traffic disruption in the fabric.

Recommended Action

First, collect a supportsave and contact the switch vendor for analysis. If the number of requested buffers by the port is unexpectedly large, and if the port is a frontend port, toggle the identified port using portdisable, portenable, portcfgpersistentdisable, or portcfgpersistentenable. If that doesn't work, or if the port is a backend port, use slotpoweroff and slotpoweron on the identified blade. If the number of requested buffers makes sense and the current total ASIC buffers is very close to the ASIC maximum, contact the switch vendor to analyze switch data for possible ports to toggle and the next actions to take on the switch.

GE5-1049

Message

S<Slot number>,P<User port index>(<Blade port number>): Port faulted at <String to identify location>. Requested <Maximum possible buffers> buffers; ASIC buffers: current=<Desired buffer count on the one port> max=<Total Number of buffers desired on ASIC>

Message Type

LOG | FFDC

Message Severity

ERROR

Probable Cause

More buffers have been requested/desired than exist on the ASIC. This will cause traffic disruption in the fabric.

Recommended Action

if the number of requested buffers by the port is unexpectedly large, and if the port is a frontend port, toggle the identified port using portdisable, portenable, portcfgpersistentdisable, or portcfgpersistentenable. If that doesn't work, or if the port is a backend port, use slotpoweroff and slotpoweron on the identified blade. If the number of requested buffers makes sense and the current total ASIC buffers is very close to the ASIC maximum, contact the switch vendor to analyze switch data for possible ports to toggle and the next actions to take on the switch.

GE5-1050

Message

S<Slot number>,C<Chip index>: No buffers allocated to <String to specify type of port> port. Requested <Maximum possible buffers> buffers; ASIC buffers: current=<Desired buffer count on the one port> max=<Total Number of buffers desired on ASIC>

Message Type

LOG | FFDC

Message Severity

ERROR

Probable Cause

More buffers have been requested/desired than exist on the ASIC. This will cause traffic disruption in the fabric.

Recommended Action

First, take a supportsave and contact the switch vendor for analysis. If the number of requested buffers by the port is unexpectedly large, or if the number of requested buffers makes sense and the current total ASIC buffers is very close to the ASIC maximum, contact the switch vendor to analyze switch data for possible ports to toggle and the next actions to take on the switch.

GE5-1051

Message

S<Slot number>,P<User port index>(<Blade port number>): Port desired buffer mismatch. actual: <Actual desired buffer count on the port> expected: <Expected desired buffer count on the port>

Message Type

LOG | FFDC

Message Severity

ERROR

Probable Cause

The number of buffers requested by a port does not match the number of buffers this port is supposed to request.

Recommended Action

First, collect a supportsave and contact the switch vendor. If the number of requested buffers by the port is unexpectedly large, and if the port is a frontend port, toggle the identified port using portdisable, portenable, portcfgpersistentdisable, or portcfgpersistentenable. If that doesn't work, or if the port is a backend port, use slotpoweroff and slotpoweron on the identified blade.

GE5-1052

Message

S<Slot number>,C<Chip index>: <String to specify type of port> port desired buffer mismatch. actual: <Actual desired buffer count on the port> expected: <Expected desired buffer count on the port>

Message Type

LOG | FFDC

Message Severity

ERROR

Probable Cause

The number of buffers requested by a port does not match the number of buffers this port is supposed to request.

Recommended Action

First, take a supportsave and contact the switch vendor for analysis. If the number of requested buffers by the port is unexpectedly large, contact the switch vendor to analyze switch data for the next actions to take on the switch.

GE5-1053

Message

S<slot number>,P<port number>(<blade port number>): 4G Speed is supported for F-Port only.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the E-Port is operating at 4G speed. The 4G speed is supported only on F_Ports.

Recommended Action

GE5-1054

Message

S<slot number>,P<port number>(<blade port number>): Media initialization fault; please reseal or replace media
rtryctr:<retries left>/<max retries > rate:<High(2)/Low rate(1)> failure:<failure code>.

Message Type

LOG | FFDC

Message Severity

ERROR

Probable Cause

A Media initialization fault occurs because the media is not seated properly or the SFP is faulty.Actions such as media plug-out/plug-in and switch power-cycle can cause this fault.

Recommended Action

Follow these steps: 1. Disable the port, and then enable it. 2. Reseat the media. 3. If reseating does not recover the module, replace the module.

GE5-1055

Message

Port in Slot <slot number>, Port <port number>(<blade port number>) getting faulted with reason <port fault reason>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the port has faulted because of errors.

Recommended Action

Disable and enable the port, and if the problem persists, replace the blade.

GE5-1056**Message**

Chip in Slot <slot number>, Chip <chip index> getting faulted with reason <Fault reason>.

Message Type

LOG

Message Severity

CRITICAL

Probable Cause

Indicates that above-normal errors were observed in the hardware and the chip has faulted.

Recommended Action

When this error is observed persistently, power-cycle the specified blade using the `slotPowerOff` and `slotPowerOn` commands. If the problem persists, replace the blade.

GE5-1057**Message**

S<slot number>,C<chip index>: HW ASIC Chip is in an inconsistent state = 0x<chip error>.

Message Type

LOG

Message Severity

CRITICAL

Probable Cause

Indicates that an internal error has been observed in the application-specific integrated circuit (ASIC) hardware that may degrade the data traffic.

Recommended Action

To recover a bladed system, execute the slotPowerOff and slotPowerOn commands on the blade. To recover a nonbladed system, execute the fastBoot command on the switch at the next customer maintenance window.

HAM Messages

HAM module error messages.

HAM-1001

Message

Standby CP is not healthy, device <device name> status BAD, Severity = <severity level>.

Message Type

FFDC | LOG

Message Severity

CRITICAL

Probable Cause

Indicates that a standby control processor (CP) device error is reported by the high availability manager (HAM) health monitor, with the specified device and severity level. The severity level can be critical, major, or minor.

The active CP will continue to function normally. Because the standby CP is not healthy, non-disruptive failover is not possible.

Recommended Action

Restart the standby CP blade by ejecting the card and reseating it. If the problem persists, replace the standby CP.

HAM-1002

Message

Standby CP is healthy.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that all standby control processor (CP) devices monitored by the high availability manager (HAM) health monitor reported no error.

HAM-1004**Message**

Processor rebooted - <Reboot Reason>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the switch has been restarted because of a user action or an error. The switch restart can be initiated by the `firmwareDownload`, `fastBoot`, `haFailover`, and `reboot` commands. Some examples of errors that may initiate this message are hardware errors, software errors, compact flash errors, or memory errors. The *Reboot Reason* variable can be one of the following:

- Hafaileover
- Reset
- Fastboot
- Giveup Master:SYSM
- CP Faulty:SYSM
- FirmwareDownload
- ConfigDownload:MS
- ChangeWWN:EM
- Reboot:WebTool
- Fastboot:WebTool
- Software Fault:Software Watchdog
- Software Fault:Kernel Panic
- Software Fault:ASSERT
- Reboot:SNMP
- Fastboot:SNMP
- Reboot
- Chassis Config
- Reboot:API
- Reboot:HAM
- EMFault:EM

Recommended Action

Execute the `errShow` command on both control processors (CPs) to view the error log for additional messages that may indicate reason for the switch restart.

HAM-1005

Message

HeartBeat Miss reached threshold.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that either the active CP Ethernet Media Access Controller (EMAC) or the standby CP is down. The active CP will run a diagnostic test on EMAC and will wait for the standby CP to reset it if it is down.

HAM-1006

Message

EMAC controller for Active CP is BAD.

Message Type

FFDC | LOG

Message Severity

CRITICAL

Probable Cause

Indicates that the local Ethernet Media Access Controller (EMAC) on the active CP has been marked BAD as determined by the diagnostic test run by the high availability manager (HAM) module.

Recommended Action

The standby CP will take over and reset the active CP. The system will be non-redundant because the standby CP becomes the active CP.

HAM-1007

Message

Need to reboot the system for recovery, reason: <reason name>.

Message Type

FFDC | LOG

Message Severity

CRITICAL

Probable Cause

Indicates that the switch in current condition needs to be restarted to achieve a reliable recovery. The reasons can be one of the following:

- The standby CP was not ready when failover occurred.
- The failover occurred when the last logical switch (LS) transaction was incomplete.
- The switch failed when timeout occurred at certain stage.
- The cold or warm recovery has failed.

Recommended Action

If auto-reboot is enabled, the switch will automatically restart. Otherwise, execute the `reboot` command to manually restart the switch.

HAM-1008

Message

Rebooting the system for recovery - auto-reboot is enabled.

Message Type

FFDC | LOG

Message Severity

CRITICAL

Probable Cause

Indicates that the recovery by auto-reboot is enabled, and therefore the switch automatically restarts. This message is displayed if the event logged in HAM-1007 has occurred and auto-reboot is enabled.

Recommended Action

Wait until the switch is up to perform any operations.

HAM-1009

Message

Need to MANUALLY REBOOT the system for recovery - auto-reboot is disabled.

Message Type

FFDC | LOG

Message Severity

CRITICAL

Probable Cause

Indicates that the recovery by auto-restart is disabled, therefore the switch needs to be manually restarted for recovery. This message is displayed if the event logged in HAM-1007 has occurred and auto-reboot is disabled.

Recommended Action

Execute the `reboot` command to restart the switch manually.

HAM-1010

Message

Manually trigger `haReboot/reboot` for recovery from OOM when appropriate.

Message Type

LOG

Message Severity

CRITICAL

Probable Cause

Indicates that out of memory (OOM) condition has been detected when the switch was not ready for warm recovery.

Recommended Action

Manually trigger the switch restart for cold recovery, if needed; or wait until switch is ready for warm recovery and execute the `haReboot` or `haFailover` command.

HAM-1011

Message

`haReboot` is automatically triggered for warm recovery from OOM.

Message Type

FFDC | LOG

Message Severity

CRITICAL

Probable Cause

Indicates that out of memory (OOM) condition has been detected when switch was ready for warm recovery. The `haReboot` is automatically triggered.

Recommended Action

No action is required. The `haReboot` is automatically triggered to recover from the OOM condition.

HAM-1013

Message

<error message>.

Message Type

LOG

Message Severity

CRITICAL

Probable Cause

Indicates that the software watchdog has detected termination of a restartable daemon, but could not restart the daemon.

Recommended Action

Manually initiate a restart or failover, if needed.

HAM-1014

Message

<error message>.

Message Type

LOG

Message Severity

CRITICAL

Probable Cause

Indicates that the software watchdog has detected termination of a restartable daemon and needs to restart or initiate a failover.

Recommended Action

Execute the `reboot` command to restart the system or initiate a failover by using the `haFailover` command.

HAM-1015

Message

<info message>.

Message Type

AUDIT

Message Class

RAS

Message Severity

INFO

Probable Cause

Indicates that a terminated software component has been restarted.

HAM-1016

Message

Invalid Dexansion request: <reason name>.

Message Type

FFDC | LOG

Message Severity

CRITICAL

Probable Cause

Indicates that the active CP has sent an invalid dexansion request.

Recommended Action

HASM collects the required logs and skips the invalid request. This helps to keep the daemon alive by skipping the invalid request causing the hasmd to crash

HAM-1017

Message

High Availability <Enabled or Disabled>.

Message Type

AUDIT

Message Class

RAS

Message Severity

INFO

Probable Cause

Indicates that the High Availability is disabled or enabled.

HAM-1018**Message**

HA Reboot.

Message Type

AUDIT

Message Class

RAS

Message Severity

INFO

Probable Cause

Indicates that the CLI HA reboot triggered.

HAM-1019**Message**

Standby CP FOS is not enabled due to CP Mismatch.

Message Type

LOG

Message Severity

CRITICAL

Probable Cause

Indicates that FOS bringup is disabled on Standby CP.

Recommended Action

Insert a new Standby CP.

HAM-1020**Message**

Rebooting Standby CP to recover.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that FOS bringup failed on Standby CP.

HAM-1021

Message

The Blade-ID has changed in slot <slot number> from <old blade-id> to <current blade-id>.

Message Type

LOG

Message Severity

CRITICAL

Probable Cause

Indicates that blade-id has changed compared to older blade.

Recommended Action

Execute `slotcfg --default -reset slot_number#` command to recover the faulty blade.

HAMK Messages

High Availability Management (HAM) daemon error messages.

HAMK-1001

Message

Warm Recovery Failed.

Message Type

LOG | FFDC

Message Severity

CRITICAL

Probable Cause

Indicates that the switch failed during the warm recovery.

Recommended Action

This event triggers the switch restart automatically and attempts a cold recovery.

Execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

HAMK-1002**Message**

Heartbeat down.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the active control processor (CP) blade determined that the standby CP blade is down. This can be a result of a user-initiated action such as firmware download, the standby CP blade being reset or removed, or an error in the standby CP blade.

Recommended Action

Monitor the standby CP blade for a few minutes. If this message is due to a standby CP restart, the HAMK-1003 message will display after the standby CP is restarted.

If the standby CP does not connect to the active CP after 10 minutes, restart the standby CP blade by ejecting the blade and reseating it.

HAMK-1003**Message**

Heartbeat up.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the active control processor (CP) blade detected the standby CP blade. This means that the standby CP blade is available to take over in case a failure happens in the active CP blade. Typically, this message is displayed when the standby CP blade restarts.

HAMK-1004

Message

Resetting standby CP (double reset may occur).

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the standby control processor (CP) is being reset due to a loss of heartbeat. Typically, this message is displayed when the standby CP has been restarted. Note that in certain circumstances, a CP may experience a double reset and restart twice. A CP can recover automatically even if it has restarted twice.

HIL Messages

Hardware independent layer error messages.

HIL-1101

Message

Slot <slot number> faulted, <nominal voltage> (<measured voltage>) is above threshold.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the blade voltage is above threshold.

Recommended Action

Replace the faulty blade or switch (for non-bladed switches).

HIL-1102

Message

Slot <slot number> faulted, <nominal voltage> (<measured voltage>) is below threshold.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the blade voltage is below threshold.

Recommended Action

Replace the faulty blade or switch (for non-bladed switches).

HIL-1103

Message

Blower <blower number> faulted, <nominal voltage> (<measured voltage>) is above threshold.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the fan voltage is above threshold.

Recommended Action

Run the `psShow` command to verify the power supply status.

Try to reseat the faulty fan field-replaceable units (FRUs) and power supply FRU to verify that they are seated properly.

If the problem persists, replace the fan FRU or the power supply FRU as necessary.

HIL-1104

Message

Blower <blower number> faulted, <nominal voltage> (<measured voltage>) is below threshold.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the fan voltage is below threshold.

Recommended Action

Run the `psShow` command to verify the power supply status.

Try to reseal the faulty fan field-replaceable units (FRUs) and power supply FRU to verify that they are seated properly.

If the problem persists, replace the fan FRU or the power supply FRU as necessary.

HIL-1105**Message**

Switch error, <nominal voltage> (<measured voltage>) above threshold.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the switch voltage is above threshold. This message is specific to non-bladed switches.

Recommended Action

For switches that do not have field-replaceable units (FRUs), replace the entire switch.

If the 12 volt level is faulty, replace one or both power supplies; if any other voltage is faulty, replace the entire switch.

HIL-1106**Message**

Switch error, <nominal voltage> (<measured voltage>) below threshold.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the switch voltage is below threshold. This message is specific to non-bladed switches.

Recommended Action

For switches that do not have field-replaceable units (FRUs), replace the entire switch.

If the 12 volt level is faulty, replace one or both power supplies; if any other voltage is faulty, replace the entire switch.

HIL-1107**Message**

Switch faulted, <nominal voltage> (<measured voltage>) above threshold. System preparing for reset.

Message Type

FFDC | LOG

Message Severity

CRITICAL

Probable Cause

Indicates that the switch voltage is above threshold. This message is specific to non-bladed switches.

Recommended Action

For switches that do not have field-replaceable units (FRUs), replace the entire switch.

If the 12 volt level is faulty, replace one or both power supplies; if any other voltage is faulty, replace the entire switch.

HIL-1108**Message**

Switch faulted, <nominal voltage> (<measured voltage>) below threshold. System preparing for reset.

Message Type

FFDC | LOG

Message Severity

CRITICAL

Probable Cause

Indicates that the switch voltage is below threshold. This message is specific to non-bladed switches.

Recommended Action

For switches that do not have field-replaceable units (FRUs), replace the entire switch.

If the 12 volt level is faulty, replace one or both power supplies; if any other voltage is faulty, replace the entire switch.

HIL-1109

Message

PS <Power Supply Number 1..4> SEEPROM corruption (fruhdr checksum mismatch) detected.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates detection of Power Supply (PS) Field Replaceable Unit header (fruhdr) checksum mismatch.

Recommended Action

No action is required. The checksum mismatch is benign.

HIL-1201

Message

Blower <blower number>, speed (<measured speed> RPM) above threshold.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the fan speed (in RPM) has risen above the maximum threshold. A high speed does not necessarily mean that the fan is faulty.

Recommended Action

Run the `tempShow` command to verify that the switch temperatures are within operational ranges. Refer to the hardware reference manual for the temperature range of your switch.

Make sure that the area is well-ventilated and that the room temperature is within the operational range of your switch. Refer to the hardware reference manual for your switch for the operational temperature range.

Run the `fanShow` command to monitor the speed of the fan generating this error.

If the fan continues to generate this message, replace the fan FRU.

HIL-1202

Message

Blower <blower number> faulted, speed (<measured speed> RPM) below threshold.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the specified fan speed (in RPM) has fallen below the minimum threshold.

Recommended Action

Replace the fan FRU.

HIL-1203

Message

Fan <fan number> faulted, speed (<measured speed> RPM) above threshold.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the specified fan speed (in RPM) has risen above the maximum threshold. A high speed does not necessarily mean that the fan is faulty.

Recommended Action

Run the `tempShow` command to verify that the switch temperatures are within operational ranges. Refer to the hardware reference manual for the temperature range of your switch.

Make sure that the area is well-ventilated and that the room temperature is within the operational range of your switch. Refer to the hardware reference manual for your switch for the operational temperature range.

Run the `fanShow` command to monitor the speed of the fan generating this error.

If the fan continues to generate this message, replace the fan FRU.

HIL-1204

Message

Fan <fan number> faulted, speed (<measured speed> RPM) below threshold.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the specified fan speed (in RPM) has fallen below the minimum threshold. This message is specific to non-bladed switches.

Recommended Action

Replace the fan field-replaceable unit (FRU).

For switches that do not have FRUs, replace the entire switch.

HIL-1206

Message

Fan <fan number> sensor <sensor number> , speed (<measured speed> RPM) below threshold.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the specified fan speed (in RPM) has fallen below the minimum threshold. This problem can quickly cause the switch to overheat. This message is specific to non-bladed switches.

Recommended Action

Replace the fan field-replaceable unit (FRU), where applicable. For non-FRU components, please contact your equipment vendor's support.

HIL-1207

Message

Fan <fan number> is faulty.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the fan is faulty.

Recommended Action

Use the `tempShow` command to verify that the switch temperatures are within operational ranges. Refer to the hardware reference manual for the temperature range of your switch.

Make sure that the area is well-ventilated and that the room temperature is within the operational range of your switch. Refer to the hardware reference manual for your switch for the operational temperature range.

Use the `fanShow` command to monitor the status of the fan generating this error.

If the fan continues to generate this message, replace the switch because the fan is not field-replaceable.

HIL-1208

Message

Fan <fan number> is not faulty.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the fan is not faulty.

Recommended Action

This can only occur on switches with non-removable fans. It follows a previous indication of faultiness.

If the fan continues to generate this message, it indicates oscillation between faulty and non-faulty behavior. Replace the switch because the fan is not field-replaceable.

HIL-1301

Message

1 blower failed or missing. Replace failed or missing blower assembly immediately.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that a fan field-replaceable unit (FRU) has failed or has been removed. This message is often preceded by a low speed error message. This problem can cause the switch to overheat.

Recommended Action

Replace the affected fan FRU immediately.

HIL-1302**Message**

<count> blowers failed or missing. Replace failed or missing blower assemblies immediately.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that multiple fan field-replaceable units (FRUs) have failed or are missing on a switch. This message is often preceded by a low fan speed message.

Recommended Action

Replace the affected fan FRUs immediately.

HIL-1303**Message**

One fan failed. Replace failed fan FRU immediately.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that a fan field-replaceable unit (FRU) has failed. This message is often preceded by a low fan speed message.

Recommended Action

Replace the faulty fan FRU immediately.

HIL-1304**Message**

Two fans failed. Replace failed fan FRUs immediately.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that multiple fan field-replaceable units (FRUs) have failed. This message is often preceded by a low fan speed message.

Recommended Action

Replace the faulty fan FRUs immediately.

HIL-1305**Message**

One or two fans failed. Replace failed fan FRUs immediately.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that multiple fan field-replaceable units (FRUs) have failed. This message is often preceded by a low fan speed message.

Recommended Action

Replace the faulty fan FRUs immediately.

HIL-1306

Message

Three fans failed. Replace failed fan FRUs immediately.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that three fan field-replaceable units (FRUs) have failed. This message is often preceded by a low fan speed message.

Recommended Action

Replace the faulty fan FRUs immediately.

HIL-1307

Message

Four or five fans failed. Replace failed fan FRUs immediately.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that multiple fan field-replaceable units (FRUs) have failed. This message is often preceded by a low fan speed message.

Recommended Action

Replace the faulty fan FRUs immediately.

HIL-1308

Message

All fans failed. Replace failed fan FRUs immediately.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that all fans have failed. This message is often preceded by a low fan speed message.

Recommended Action

Replace the faulty fan field-replaceable units (FRUs) immediately.

HIL-1309**Message**

<count> fan FRUs failed. Replace failed fan FRUs immediately.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that multiple fans have failed. This message is often preceded by a low fan speed message.

Recommended Action

Replace the faulty fan field-replaceable units (FRUs) immediately.

HIL-1310**Message**

<count> fan(s) faulty.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that multiple fans have failed. This message is often preceded by a low fan speed message.

Recommended Action

Because the fans are not field-replaceable, replace the switch if the temperature is high.

HIL-1311**Message**

No fans are faulty.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates recovery from an earlier condition of one or more fans having failed.

Recommended Action

This can only occur on switches with non-removable fans. It follows a previous indication of faultiness.

If the fan continues to generate this message, it indicates oscillation between faulty and non-faulty behavior. Replace the switch because the fan is not field-replaceable.

HIL-1312**Message**

<number of failed fans> blower(s) failed. Check all blower units immediately.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that one or more fan or blower units have failed on the switch. This message is often preceded by a low fan speed or fan failure message.

Recommended Action

Check the `fanShow` command to see the system operating temperatures. Ensure the system is within operational temperature limits and the system has adequate airflow.

If fans are present and spinning but marked as faulty or missing, rebooting the switch may be necessary.

Please contact your equipment vendor's support.

HIL-1401

Message

One fan FRU missing. Install fan FRU immediately.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that a fan field-replaceable unit (FRU) has been removed.

Recommended Action

Install the missing fan FRU.

HIL-1402

Message

Two fan FRUs missing. Install fan FRUs immediately.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that two fan field-replaceable units (FRUs) have been removed.

Recommended Action

Install the missing fan FRUs immediately.

HIL-1403

Message

All fan FRUs missing. Install fan FRUs immediately.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that all fan field-replaceable units (FRUs) have been removed.

Recommended Action

Install the missing fan FRUs immediately.

HIL-1404**Message**

<count> fan FRUs missing. Install fan FRUs immediately.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that one or more fan field-replaceable units (FRUs) have been removed.

Recommended Action

Install the missing fan FRUs immediately.

HIL-1405**Message**

<number of missing fans> fan(s) missing. Check all fans immediately.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that one or more of the expected fan units have not been detected in the system.

Recommended Action

Check the switch's fan units to ensure all are present and running.

Check the `fanShow` command to ensure system is operating within thermal thresholds. Ensure the system has adequate airflow.

Please contact your equipment vendor's support.

HIL-1501

Message

Slot <slot number>, high temperature (<measured temperature>).

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the temperature of this blade has risen above the warning threshold.

Recommended Action

Run the `fanShow` command to verify all the fans are working properly.

Make sure that the area is well-ventilated and that the room temperature is within operational range of your switch. Refer to the hardware reference manual for your switch for the operational temperature range.

HIL-1502

Message

Slot <slot number>, high temperature (<measured temperature>). Unit will be shut down in 2 minutes if temperature remains high.

Message Type

FFDC | LOG

Message Severity

CRITICAL

Probable Cause

Indicates that the temperature of this blade has risen above the critical threshold. This usually follows a high-temperature message.

Recommended Action

Run the `fanShow` command to verify all the fans are working properly.

Make sure that the area is well-ventilated and that the room temperature is within operational range of your switch. Refer to the hardware reference manual for your switch for the operational temperature range.

If the message persists, replace the blade.

HIL-1503

Message

Slot <slot number>, unit shutting down.

Message Type

FFDC | LOG

Message Severity

CRITICAL

Probable Cause

Indicates that the temperature of this blade has been above the maximum threshold for at least two minutes. The blade is shut down to prevent damage. This usually follows a high-temperature warning message.

Recommended Action

Run the `fanShow` command to verify all the fans are working properly.

Make sure that the area is well-ventilated and that the room temperature is within the operational range of your switch. Refer to the hardware reference manual for your switch for the operational temperature range.

If the message persists, replace the faulty blade.

HIL-1504

Message

System within normal temperature specifications (<measured temperature> C).

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that temperatures in the system have returned to normal.

HIL-1505

Message

High temperature (<measured temperature> C), fan speed increasing per environmental specifications.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that temperatures in the system have risen above the warning threshold and that the fan speed is being increased.

Recommended Action

Run the `fanShow` command to verify all the fans are working properly.

Make sure that the area is well-ventilated and that the room temperature is within the operational range of your switch. Refer to the hardware reference manual for your switch for the operational temperature range.

HIL-1506

Message

High temperature (<measured temperature> C) exceeds system temperature limit. System will shut down within 2 minutes.

Message Type

FFDC | LOG

Message Severity

CRITICAL

Probable Cause

Indicates that temperatures in the system have risen above the critical threshold.

Recommended Action

Run the `fanShow` command to verify that all fans are working properly. Replace any deteriorating fan field-replaceable units (FRUs), where applicable. For any deteriorating fan units that are non-FRUs, please contact your equipment vendor's support.

Make sure that the area is well-ventilated and that the room temperature is within the operational range of your switch. Refer to the hardware reference manual for your switch for the operational temperature range.

HIL-1507

Message

High temperature warning time expired. System preparing for shutdown.

Message Type

FFDC | LOG

Message Severity

CRITICAL

Probable Cause

Indicates that temperatures in the system have risen above the critical threshold.

Recommended Action

To avoid causing damage to the switch, the system shuts down automatically. To help prevent future problems, make sure that all the fans are working properly.

Make sure that the area is well-ventilated and that the room temperature is within the operational range of your switch. Refer to the hardware reference manual for your switch for the operational temperature range.

HIL-1508

Message

Fan faulty warning time expired. System preparing for shutdown.

Message Type

FFDC | LOG

Message Severity

CRITICAL

Probable Cause

Indicates that temperatures in the system have remained above the critical threshold too long.

Recommended Action

To avoid causing damage to the switch, the system shuts down automatically. To help prevent future problems, make sure that all the fans are working properly.

Make sure that the area is well-ventilated and that the room temperature is within the operational range of your switch. Refer to the hardware reference manual for your switch for the operational temperature range.

HIL-1509

Message

High temperature (<measured temperature> C). Warning time expired. System preparing for shutdown.

Message Type

FFDC | LOG

Message Severity

CRITICAL

Probable Cause

Indicates that temperatures in the system have risen above the critical threshold.

Recommended Action

To avoid causing damage to the switch, the system shuts down automatically. To help prevent future problems, make sure that all the fans are working properly.

Make sure that the area is well-ventilated and that the room temperature is within the operational range of your switch. Refer to the hardware reference manual for your switch for the operational temperature range.

HIL-1510

Message

Current temperature is below shutdown threshold. System shutdown canceled.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that temperatures in the system have dropped below the critical threshold; the system can continue operation.

Recommended Action

To help prevent future problems, make sure that all the fans are working properly.

Make sure that the area is well-ventilated and that the room temperature is within the operational range of your switch. Refer to the hardware reference manual for your switch for the operational temperature range.

HIL-1511

Message

Fan speed of all the fan FRUs is increasing to <Fan RPM> RPM as per environmental specifications.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that temperatures in the system have risen above the warning threshold and that the fan speed is being increased.

Recommended Action

Run the `fanShow` command to verify all the fans are working properly.

Make sure that the area is well-ventilated and that the room temperature is within the operational range of your switch. Refer to the hardware reference manual for your switch for the operational temperature range.

HIL-1512

Message

High temperature (<measured temperature> C), Exceeds environmental specifications.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that temperatures in the system have risen above the warning threshold.

Recommended Action

Run the `fanShow` command to verify all the fans are working properly.

Make sure that the area is well-ventilated and that the room temperature is within the operational range of your switch. Refer to the hardware reference manual for your switch for the operational temperature range.

HIL-1513

Message

Slot <slot number>, high temperature (<measured temperature>). Blade in the slot will be shut down if temperature remains high.

Message Type

FFDC | LOG

Message Severity

CRITICAL

Probable Cause

Indicates that the temperature of this blade has risen above the critical threshold. This usually follows a high-temperature message.

Recommended Action

Run the `fanShow` command to verify all the fans are working properly.

Make sure that the area is well-ventilated and that the room temperature is within operational range of your switch. Refer to the hardware reference manual for your switch for the operational temperature range.

If the message persists, replace the blade.

HIL-1514

Message

Blade in slot <slot number> is shutting down.

Message Type

FFDC | LOG

Message Severity

CRITICAL

Probable Cause

Indicates that the temperature of this blade has been above the maximum threshold for at least two minutes. The blade is shut down to prevent damage. This usually follows a high-temperature warning message.

Recommended Action

Run the `fanShow` command to verify all the fans are working properly.

Make sure that the area is well-ventilated and that the room temperature is within the operational range of your switch. Refer to the hardware reference manual for your switch for the operational temperature range.

If the message persists, replace the faulty blade.

HIL-1515

Message

High temperature (<measured temperature> C) exceeds system temperature limit. System will shutdown soon.

Message Type

FFDC | LOG

Message Severity

CRITICAL

Probable Cause

Indicates that temperatures in the system have risen above the critical threshold.

Recommended Action

Run the `fanShow` command to verify that all fans are working properly. Replace any deteriorating fan field-replaceable units (FRUs).

Make sure that the area is well-ventilated and that the room temperature is within the operational range of your switch. Refer to the hardware reference manual for your switch for the operational temperature range.

HIL-1516

Message

Fan speed of all the fan FRUs is increasing to <Fan RPM> RPM as per environmental specifications.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that temperatures in the system have risen and the fan speed is being increased.

Recommended Action

Run the `fanShow` command to verify all the fans are working properly.

Make sure that the area is well-ventilated and that the room temperature is within the operational range of your switch. Refer to the hardware reference manual for your switch for the operational temperature range.

HIL-1517

Message

Fan speed of all the fan FRUs changing to <Fan RPM> RPM as per environmental specifications.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that temperatures in the system have fallen and the fan speed is being decreased.

Recommended Action

Run the `fanShow` command to verify all the fans are working properly.

HIL-1518

Message

<number of failed and/or absent fans> failed and/or absent fan(s) exceeds system threshold. System will shut down within 2 minutes.

Message Type

FFDC | LOG

Message Severity

CRITICAL

Probable Cause

Indicates that the system has exceeded its operational limits for the allowed number of failed, faulty, and absent fan units.

Recommended Action

Run the `fanShow` command to see which fans have failed or are absent.

Make sure that the area is well-ventilated and that the room temperature is within the operational range of your switch. Refer to the hardware reference manual for your switch for the operational temperature range.

Contact your equipment vendor's support.

HIL-1519

Message

<number of failed/faulty and absent fan> failed and/or absent fans is back within system thresholds. System shutdown canceled.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the number of failed, faulty, and absent fan units has returned to be within range for the system's operational threshold.

Recommended Action

Run the `fanShow` command to verify that all fans are working properly.

Make sure that the area is well-ventilated, the fans are not blocked, and that the room temperature is within the operational range of your switch. Refer to the hardware reference manual for your switch for the operational temperature range.

If any fans are still faulty or absent, contact you equipment vendor's support.

HIL-1601

Message

Using backup temperature sensor. Attention needed.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that temperature readings from the primary sensor are out of range.

Recommended Action

Run the `fanShow` command to verify that all fans are operating correctly. Replace any deteriorating fan field-replaceable units (FRUs), where applicable. For failures in non-FRU components, please contact your equipment vendor's support.

Run the `tempShow` command to verify temperature values. If any sensor is too high, monitor the switch. Try rebooting or power cycling the switch.

HIL-1602

Message

Multiple temperature sensors failed. Service immediately.

Message Type

FFDC | LOG

Message Severity

CRITICAL

Probable Cause

Indicates that temperature readings from multiple sensors are out of range.

Recommended Action

Run the `fanShow` command to verify that all fans are operating correctly. Replace any deteriorating fan field-replaceable units (FRUs), where applicable. For failures of non-FRU components, please contact your equipment vendor's support.

Run the `tempShow` command to verify temperature values. If any sensor is too high, monitor the switch. Try rebooting or power cycling the switch.

HIL-1603

Message

<failure count> fans out of service. System is shutting down immediately.

Message Type

FFDC | LOG

Message Severity

CRITICAL

Probable Cause

Indicates that the total fan failure count is greater than or equal to two.

Recommended Action

To avoid causing damage to the switch, the system shuts down automatically. To help prevent future problems, make sure that all the fans are working properly.

HIL-1605

Message

High temperature (<measured temperature> C), fan speed increasing per environmental specifications.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that temperatures in the system have risen above the threshold and that the fan speed is being increased.

HIL-1610**Message**

Fan/PS unit <Combo fan/power supply unit number> not supplying power, fan speeds may not be available. Please ensure that the unit has power and the switch is on.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the power supply is not connected to a power source, is not switched on, or the unit is faulty.

Recommended Action

Ensure that the power cord is connected to the unit with a valid power source and then switch on the unit (if applicable). If the problem persists, try reseating the unit. If the problem still persists, replace the FRU.

HIL-1611**Message**

MISMATCH in PSU-FAN Air Flow direction. Replace PSU with fan air flows in same direction. System will be shut down in 2 minutes.

Message Type

FFDC | LOG

Message Severity

CRITICAL

Probable Cause

Indicates that the airflows of the power supply and fan assemblies are moving in the reverse or opposite direction, which could overheat the system. The airflow of the power supply and fan assemblies must move in the same direction or the system will shut down in two minutes.

Recommended Action

Use the `chassisShow` command to check the airflow directions of the power supply and fan assemblies. Ensure that the airflows run in the same direction.

HIL-1612**Message**

MISMATCH in PSU-FAN Air Flow direction. System shut down.

Message Type

LOG

Message Severity

CRITICAL

Probable Cause

Indicates that the airflows of the power supply and fan assemblies are moving in the reverse or opposite direction. The system will shut down immediately.

Recommended Action

Ensure that the airflows of the power supply and fan assemblies run in the same direction.

HIL-1613**Message**

PSU-FAN FRUS Air Flow matched. System shutdown canceled.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the airflows of the power supply and fan assemblies have changed to move in the same direction. The system continues to operate.

Recommended Action

Ensure that the airflows of the power supply and fan assemblies run in the same direction.

HIL-1614**Message**

MISMATCH in Fan airflow direction. Replace FRU with fan airflow in same direction.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the airflow of the fan is in the reverse direction. This may heat up the system.

Recommended Action

Replace the fan field-replaceable units (FRUs) in such a manner that the air flows in the same direction as the remaining fans. Refer to the *Hardware Reference Manual* of your switch for instructions to replace the fan FRUs.

HIL-1615**Message**

MISMATCH in PSU-Fan FRUs airflow direction. Replace PSU with fan airflow in same direction.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the airflow of the power supply unit (PSU) fan is in the reverse direction. This may heat up the system.

Recommended Action

Replace the PSU fan field-replaceable unit (FRU) in such a manner that the air flows in the same direction as the remaining fans. Refer to the *Hardware Reference Manual* of your switch for instructions to replace the PSU fan FRU.

HIL-1621

Message

MISMATCH in PSU-FAN Air Flow direction. Please ensure that all fans (PSU and standalone) blow in the same direction.

Message Type

FFDC | LOG

Message Severity

WARNING

Probable Cause

Indicates that the airflows of the power supply fan assemblies are mismatched. This can lead to overheating of the system. The airflow of the power supply fan assemblies must be in the same direction as that of the standalone fan field-replaceable units (FRUs).

Recommended Action

Use the `chassisShow` command to check the airflow directions of the power supply and fan assemblies. Ensure that the airflows run in the same direction for power supply fans as well as standalone fan FRUs.

HIL-1623

Message

Airflow for the PSU-FANs and Standalone FAN FRUs is now matched.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the airflows of the power supply fans and standalone fan field-replaceable units (FRUs) are now matched and flowing in the same direction.

Recommended Action

Ensure that the airflows of the power supply fans and standalone fan FRUs run in the same direction.

HIL-1624

Message

MISMATCH in Standalone FAN FRUs Air Flow direction. Please ensure that all fans (PSU and standalone) blow in the same direction.

Message Type

FFDC | LOG

Message Severity

WARNING

Probable Cause

Indicates that the airflows of the standalone fan assemblies are mismatched. This can lead to overheating of the system. The airflow of the standalone fan assemblies must be in the same direction as that of the power supply unit (PSU) fans.

Recommended Action

Use the `chassisShow` command to check the airflow directions of the power supply and fan assemblies. Ensure that the airflows run in the same direction for power supply fans as well as standalone fan FRUs.

HIL-1625**Message**

MISMATCH in Air Flow direction between PSU-FANs and standalone FANs. Ensure that the airflow for PSU-FANs and standalone FANs match.

Message Type

FFDC | LOG

Message Severity

WARNING

Probable Cause

Indicates that the airflows of the power supply fans and standalone fan field-replaceable units (FRUs) are mismatched. This can lead to overheating of the system. The airflow of the power supply fan assemblies must be in the same direction as that of the standalone fan FRUs.

Recommended Action

Use the `chassisShow` command to check the airflow directions of the power supply and fan assemblies. Ensure that the airflows run in the same direction for power supply fans as well as standalone fan FRUs.

HIL-1626**Message**

Fan direction of Fan FRU unit <FAN FRU unit number> mismatches with the chassis air flow direction.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the fan direction of fan field-replaceable unit (FRU) mismatches with the chassis air flow direction programmed in the WWN cards.

Recommended Action

Replace the existing fan FRU with a fan FRU compatible with the chassis air flow direction.

HIL-1627**Message**

Fan direction of PS FRU unit <PS FRU unit number> mismatches with the chassis air flow direction.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the fan direction of power supply (PS) field-replaceable unit (FRU) mismatches with the chassis air flow direction programmed in the WWN cards.

Recommended Action

Replace the existing PS FRU with a PS FRU compatible with the chassis air flow direction.

HIL-1628**Message**

Fan direction(<Fan air flow direction>) of PSU-Fan FRU unit <PSU-Fan FRU unit number> mismatches with the system air flow direction(<System air flow direction>).

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the fan direction of PSU-Fan field-replaceable unit (FRU) mismatches with the system air flow direction.

Recommended Action

Replace the existing PSU-Fan FRU with a PSU-Fan FRU compatible with the system air flow direction.

HIL-1629**Message**

PSU unit <PS FRU unit number> input voltage(<Input Voltage>V) is in invalid range.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the PSU input voltage is not within the expected range.

Recommended Action

Check the PSU input voltage source.

HIL-1630**Message**

Auto-configuring system airflow direction to <System airflow direction>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that FOS has auto-configured system airflow direction. This usually happens when FOS identifies that the system airflow direction mismatches with the airflow direction of all fans and/or power supplies.

HIL-1650**Message**

Unable to detect <WWN Card Unit Number(s)> in chassis. Access to WWN halted.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that one or both of the World Wide Name (WWN) cards is missing. Both WWN cards must be present for normal operation.

Recommended Action

Make sure that both WWN cards are inserted.

HIL-1651**Message**

On switch/slot <Slot Id>. WWN is corrupted on both cards.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that World Wide Name (WWN) is corrupted in one or both of the WWN cards. At least one WWN card must have a valid WWN for normal operation.

Recommended Action

Contact your switch service provider for assistance.

HIL-1652**Message**

Power supply unit <UnitNumber>, Temperature (<Temperature>). Power Supply Unit will be shut down if temperature remains high.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that power supply unit temperature has risen to threshold. Power supply is going to shutdown.

Recommended Action

Run the `psshow` command to verify all power supply unit temperature.

Make sure that the area is well-ventilated and that the room temperature is within operational range of your switch. Refer to the hardware reference manual for your switch for the operational temperature range.

HIL-1653**Message**

Power supply unit <UnitNumber>, Gen5 PS is in use. Please replace it with Gen6 PS for high availability operation.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that user inserted the system with Gen5 PS and needs to be replaced.

Recommended Action

Run the `psshow` command to verify that supported power supply unit is being used.

HIL-1654**Message**

<Message string>

Message Type

FFDC | LOG

Message Severity

CRITICAL

Probable Cause

Can be caused if an integrated FRU (PS and FAN) is absent, all FRUs are faulty, airflow mismatch between FRUs or if global airflow direction in SEEPROM is not supported.

Recommended Action

To be transmitted to engineering for problem analysis.

HIL-1655

Message

<Message string>

Message Type

LOG

Message Severity

WARNING

Probable Cause

Can be caused by raising temperature in the system.

Recommended Action

Run the `fanShow` command to verify all the fans are working properly.

Make sure that the area is well-ventilated and that the room temperature is within the operational range of your switch. Refer to the *Hardware Reference Manual* for your switch for the operational temperature range.

HIL-1656

Message

FRU <FRU number> tach sensor <sensor number>, speed (<measured speed> RPM) below threshold.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the specified fan speed (in RPM) has fallen below the minimum threshold. This problem can quickly cause the switch to overheat. This message is specific to non-bladed switches.

Recommended Action

Replace the fan field-replaceable unit (FRU), where applicable. For non-FRU components, please contact your equipment vendor's support.

HIL-1657

Message

Thermal Policy changed. Long Reach Optics Thermal Policy in effect.

Message Type

LOG

Message Severity

INFO

Probable Cause

LWL or ELWL sfp connected to switch.

Recommended Action

Follow the new thermal policy.

HIL-1658**Message**

Power supply unit <UnitNumber>, 250W PS is in use. Please replace it with 350W PS for high availability operation.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that user inserted the system with 250W PS and needs to be replaced.

Recommended Action

Run the `psshow` command to verify that supported power supply unit is being used.

HIL-1659**Message**

FRU <FRU number> tach sensor <sensor number>, speed (<measured speed> RPM) above threshold.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the specified fan speed (in RPM) is above maximum threshold.

Recommended Action

Replace the fan field-replaceable unit (FRU), where applicable. For non-FRU components, please contact your equipment vendor's support.

HIL-1660**Message**

Temperature of PSU <psu number> (<measured temperature> C) exceeded threshold value.

Message Type

FFDC | LOG

Message Severity

CRITICAL

Probable Cause

Indicates that the temperature of this PSU has risen above the critical threshold.

Recommended Action

Run the `fanShow` command to verify all the fans are working properly.

Make sure that the area is well-ventilated and that the room temperature is within operational range of your switch. Refer to the hardware reference manual for your switch for the operational temperature range.

If the message persists, replace the PSU.

HLO Messages

HLO error messages.

HLO-1001**Message**

Incompatible Inactivity timeout <dead timeout> from port <port number>, correct value <value>.

Message Type

LOG | FFDC

Message Severity

ERROR

Probable Cause

Indicates that the hello (HLO) message was incompatible with the value specified in the fabric shortest path first (FSPF) protocol. The Brocade switch will not accept FSPF frames from the remote switch.

In Fabric OS, the HLO dead timeout value is not configurable, so this error can only occur when the Brocade switch is connected to a switch from another manufacturer.

Recommended Action

The dead timeout value of the remote switch must be compatible with the value specified in the FSPF protocol. Refer to the documentation for the other manufacturer's switch to change this value.

HLO-1002

Message

Incompatible Hello timeout <HLO timeout> from port <port number>, correct value <correct value>.

Message Type

LOG | FFDC

Message Severity

ERROR

Probable Cause

Indicates that the hello (HLO) message was incompatible with the value specified in the fabric shortest path first (FSPF) protocol. The Brocade switch will not accept FSPF frames from the remote switch.

In Fabric OS, the HLO timeout value is not configurable, so this error can only occur when the Brocade switch is connected to a switch from another manufacturer.

Recommended Action

The HLO timeout value of the remote switch must be compatible with the value specified in the FSPF protocol. Refer to the documentation for the other manufacturer's switch to change this value.

HLO-1003

Message

Invalid Hello received from port <port number>, Domain = <domain ID>, Remote Port = <remote port ID>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the hello (HLO) message received was invalid and the frame was dropped. The Brocade switch will not accept fabric shortest path first (FSPF) frames from the remote switch.

The switch has received an invalid HLO because either the domain or port number in the HLO message has an invalid value. This error can only occur when the Brocade switch is connected to a switch from another manufacturer.

Recommended Action

The HLO message of the remote switch must be compatible with the value specified in the FSPF protocol. Refer to the documentation for the other manufacturer's switch to change this value.

HMON Messages

Health monitor error messages.

HMON-1001

Message

<Failure description>.

Message Type

FFDC | LOG

Message Severity

CRITICAL

Probable Cause

Indicates that there was a problem reading an essential file containing configuration information from the nonvolatile storage device. This could be the result of a missing file or a corrupt file system.

Recommended Action

Execute the `firmwareDownload` command to reinstall the firmware to your switch.

If the message persists, execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

HTTP Messages

HTTP error messages.

HTTP-1001

Message

Switch PID format has changed to <current PID format>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the port ID (PID) format was changed.

Recommended Action

No action is required. For more information on PID format, refer to the *Fabric OS Administrator's Guide*.

HTTP-1002

Message

Zoning transaction initiated by User: <User Name>, Role: <User Role> completed successfully.

Message Type

AUDIT | LOG

Message Class

ZONE

Message Severity

INFO

Probable Cause

Indicates that the zoning database has been changed.

Recommended Action

Verify that the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

HTTP-1003

Message

Zoning transaction initiated by User: <User Name>, Role: <User Role> could not be completed successfully - <Reason Message>.

Message Type

AUDIT | LOG

Message Class

ZONE

Message Severity

INFO

Probable Cause

Indicates an error in completing the zoning transaction because of the specified reason.

Recommended Action

Check the ZONE events in the error message log by using the `errShow` command, and take appropriate corrective actions.

HTTP-3001

Message

REST session limit is changed to <Value>

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the maximum supported REST session limit has been changed.

HTTP-3002

Message

REST session is terminated for <User> user

Message Type

AUDIT

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates that the specified REST session has successfully terminated and logged out.

HTTP-3003**Message**

REST throttling configuration attribute, <Changed attribute>, has changed to <Value>

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the specified REST throttling configurations have been changed. The modified parameter and the new values are displayed in the message.

HTTP-3004**Message**

REST interface is <state>

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the specified REST interface has successfully enabled or disabled

HTTP-3005**Message**

REST auth key is <action>

Message Type

AUDIT | LOG

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that auth key has successfully created or deleted

HTTP-3006

Message

REST HTTP interface is <state>

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the REST HTTP interface has successfully enabled or disabled

HTTP-4001

Message

Auth mode is <state>

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the auth mode has successfully enabled or disabled

IPAD Messages

IP admin demon system messages.

IPAD-1000

Message

<Type of managed entity>/<Instance number of managed entity> <Type of network interface>/<Instance number of network interface> <Protocol address family> <Source of address change> <Value of address and prefix> <DHCP or DHCPv6 based on protocol address family> <DHCP or DHCPv6 enabled or not>.

Message Type

AUDIT | LOG

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the local IP address has been changed manually or it was reconfigured automatically by the Dynamic Host Configuration Protocol (DHCP) server.

IPAD-1001

Message

<Type of managed entity>/<Instance number of managed entity> <Protocol address family> <Source of address change> <Value of address> <DHCP or DHCPv6 based on protocol address family> <DHCP or DHCPv6 enabled or not>.

Message Type

AUDIT | LOG

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the gateway IP address has been changed manually or it was reconfigured automatically by the Dynamic Host Configuration Protocol (DHCP) server.

IPAD-1002**Message**

Switch name has been successfully changed to <Switch name>.

Message Type

AUDIT | LOG

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the switch name has been changed.

IPAD-1003**Message**

DNS parameters saved successfully.

Message Type

AUDIT | LOG

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the Domain Name System (DNS) parameters are saved successfully.

IPAD-1004**Message**

DNS parameters removed successfully.

Message Type

AUDIT | LOG

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the Domain Name System (DNS) parameters are removed successfully.

IPAD-1005

Message

Chassis name has been changed to <Chassis name>.

Message Type

AUDIT | LOG

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the chassis name has been changed.

IPAD-1006

Message

TCP timeout level has been changed to <Tcp timeout level>.

Message Type

AUDIT | LOG

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates the TCP timeout level has been changed.

IPAD-1007**Message**

IPv6 DDNS has been <DDNS is enabled or disabled>

Message Type

AUDIT | LOG

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicate the IPv6 DDNS is enabled or disabled.

ISNS Messages

ISNS server and client status messages.

ISNS-1001**Message**

Configuration peering with external iSNS server <New config iSNS server IP address> slot/port <New config Slot number>/ge<New config port number> (current <Current iSNS server IP address> <Current slot number>/ge<Current port number>).

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that a user has issued the `isnscfg` command.

ISNS-1002

Message

Start peering with external iSNS server <iSNS server IP address> slot/port <Slot number>/ge<Port number>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that peering has started with the specified external Internet Storage Name Service (iSNS) server.

ISNS-1003

Message

Peering with external iSNS server is disabled.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the IP address of the Internet Storage Name Service (iSNS) server is zero. Therefore, peering is disabled.

Recommended Action

If you wish to enable the iSNS server, use the `isnscCfg` command to show or set the server IP address; otherwise, no action is required.

ISNS-1004

Message

Timeout refreshing iSNS database with iSNS server <iSNS server IP address> slot/port <Slot number>/ge<Port number>
Reg-Period <Registration-Period in seconds>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the Internet Storage Name Service (iSNS) client fails to receive a successful response for a DevAttrQry within the specified registration period.

Recommended Action

Verify the connection of the iSNS server to the slot and port.

ISNS-1005**Message**

User request re-register with external iSNS server <iSNS server IP address> slot/port <Slot number>/ge<Port number>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that a user has requested to re-register with the specified external Internet Storage Name Service (iSNS) server.

ISNS-1006**Message**

Start re-register with external iSNS server <iSNS server IP address> slot/port <Slot number>/ge<Port number>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the re-register with the specified external Internet Storage Name Service (iSNS) server has started.

ISNS-1008**Message**

Peering with external iSNS server <iSNS server IP address> not started because configuration unchanged.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that peering with the external Internet Storage Name Service (iSNS) server was already started with the same configuration.

Recommended Action

No action is required. You may change the configuration and retry the peering with the external iSNS server.

ISNS-1009**Message**

Peering with external iSNS server <iSNS server IP address> not started because no virtual targets found.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that no virtual targets were found, and therefore peering was not started.

Recommended Action

No action is required. Peering will resume automatically when virtual targets are detected.

ISNS-1010**Message**

Slot/port <Slot>/ge<Port> is out of range.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the slot or port is out of range.

Recommended Action

Retry with a valid slot and port. Refer to the appropriate hardware reference manual for valid slot and port ranges.

ISNS-1011**Message**

iSNS Client Service is <iSNS client State (enabled/disabled)>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates the current state of the Internet Storage Name Service (iSNS) client is enabled or disabled.

Recommended Action

No action is required. Use the `fosconfig --show` command to display the current state of the iSNS client.

ISNS-1013**Message**

iSNS server connection failure.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the Internet Storage Name Service (iSNS) client failed to establish a connection with the iSNS server.

Recommended Action

Verify the connection of the iSNS server to the slot and port.

Use the `isnscfg` command to display or correct the server IP address.

ISNS-1014

Message

Start peering with external iSNS server <iSNS server IP address> on management port.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that peering has started with the specified external Internet Storage Name Service (iSNS) on the management port.

KAC Messages

KAC error messages.

KAC-1002

Message

KAC(<Key Vault Type>) communication Error: Error connecting to <Backup or Primary>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the Key Archive Client (KAC) is unable to communicate with the primary or backup key vault.

Recommended Action

Determine whether the configured key vault is operational; if not, change the switch key vault settings or resolve the operational problem at the key vault.

KAC-1004

Message

KAC <Operation Description> to Key Vault failed.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the Key Archive Client (KAC) is unable to do the specified operation to the primary or backup key vault.

Recommended Action

Determine whether the configured key vault is operational; if not, change the switch key vault settings or resolve the operational problem at the key vault.

KAC-1006

Message

Switch to Key Vault trustee link was not established.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the trustee link was not established between the switch and the key vault.

Recommended Action

Establish a trustee link between the switch and the key vault.

KAC-1007

Message

KAC key archival operation to Key Vault failed, LUN=<LUN Number>, keyID=<Key ID Value>, errno=<Error Number>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the Key Archive Client (KAC) is unable to archive the key to primary or backup key vault.

Recommended Action

Determine whether the configured key vault is operational; if not, change the switch key vault settings or resolve the operational problem at the key vault.

KAC-1008**Message**

Putting of TEP failed. Check if there is already an unapproved TEP, then delete it. Error code=<Error code from LKM>, string=<Error string>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that there was already a pending unapproved Trusted link Establishment Package (TEP) at the Lifetime Key Manager (LKM).

Recommended Action

Log in to LKM and delete the unapproved TEP.

KAC-1009**Message**

Primary(<Primary Keyvault IP Address>) and Backup(<Backup Keyvault IP Address>) Key Vaults are not in sync. Detected key mismatch with KeyID = <KeyID>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the primary and backup key vault contents are not in sync.

Recommended Action

Synchronize the contents of the primary and backup key vaults using instructions provided by the key vault provider.

KAC-1010

Message

Archival for KeyID <KeyID> failed to <Keyvault IP Address>. Error code=<Error code>, string=<Error string>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that archiving of Data Encryption Key (DEK) to the key vault failed.

KAC-1011

Message

Archival of Dummy DEK to the KV <Keyvault IP Address> failed. Dummy DEK: <Dummy Key Id>, KeyCount: <Key Count>. Error code=<Error code>, string=<Error string>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that archiving of dummy Data Encryption Key (DEK) to the key vault failed.

KAC-1012

Message

Retrieval of Dummy DEK from the KV <Keyvault IP Address> failed. Dummy DEK: <Dummy Key Id>, KeyCount: <Key Count>. Error code=<Error code>, string=<Error string>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that retrieving of dummy Data Encryption Key (DEK) from the key vault failed.

KAC-1013**Message**

Archival of the Actual DEK to the KV <Keyvault IP Address> failed. Actual Key: <Actual Key Id>. Error code=<Error code>, string=<Error string>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that archiving of actual Data Encryption Key (DEK) to the key vault failed.

KAC-1014**Message**

Retrieval of Actual DEK from the KV <Keyvault IP Address> failed. Actual Key: <Actual Key Id>. Error code=<Error code>, string=<Error string>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that retrieving of actual Data Encryption Key (DEK) from the key vault failed.

KAC-1015**Message**

KAC(<Key Vault Type>) communication Error: Error connecting to <Key Vault IP>. Error code=<Error code>, string=<Error string>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the Key Archive Client (KAC) is unable to communicate with the primary or backup key vault.

Recommended Action

Change the switch key vault settings and make sure the configured key vault is operational.

KAC-1016**Message**

Error: Key ID mismatched in request/response. Requested key ID <Key ID in response> and key in response <Requested Key Id>. Error code=<Error code>, string=<Error string>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates a mismatch between the requested key ID and the key in the response from the key vault.

Recommended Action

Determine whether the configured key vault is operational; if not, change the switch key vault settings or resolve the operational problem at the key vault.

KAC-1017**Message**

Error: KV parameter [<param name>] configured on BES is not supported by the Key Vault. Please fix the configuration of the parameter to ensure key operations function as expected.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates a mismatch between the configured key vault parameters on the Brocade Encryption Switch (BES) and the functionality supported by the key vault.

Recommended Action

De-register the key vaults, set the correct value for key vault parameter, and re-register the key vaults.

KAC-1018**Message**

KAC(<Key Vault Type>) communication to <Backup or Primary> restored.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that Key Archival Client communication with the *primary* or *backup* key vault is restored.

Recommended Action

None

KSWD Messages

Kernel software watchdog (KSWD) error messages.

KSWD-1001**Message**

<Software component>:<Software component Process ID> failed to refresh (<Current time>:<Refresh time>).

Message Type

FFDC | LOG

Message Severity

WARNING

Probable Cause

Indicates that one of the critical daemons is found to be unresponsive. An abort signal is sent.

Recommended Action

Copy the warning message along with any core file information and contact your switch service provider.

KSWD-1002

Message

Detected termination of process <Software component>:<Software component Process ID>.

Message Type

FFDC | LOG

Message Severity

WARNING

Probable Cause

Indicates that a process on the switch has ended unexpectedly.

Recommended Action

Copy the warning message along with any core file information and contact your switch service provider.

KTRC Messages

Kernel RAS trace module error messages.

KTRC-1001

Message

Dump memory size exceeds dump file size.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the dump memory size has exceeded the dump file size.

Recommended Action

Execute the `supportSave` command and reload the switch. If the problem persists, contact your switch service provider.

KTRC-1002

Message

Concurrent trace dumping.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the initial background dump has not completed.

KTRC-1003**Message**

Cannot open ATA dump device.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the advanced technology attachment (ATA) dump driver is not initialized properly.

Recommended Action

Execute the `supportSave` command and reload the switch. If the problem persists, contact your switch service provider.

KTRC-1004**Message**

Cannot write to ATA dump device.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the write boundary in the advanced technology attachment (ATA) dump device has been exceeded.

Recommended Action

Execute the `supportSave` command and reload the switch. If the problem persists, contact your switch service provider.

KTRC-1005

Message

Trace initialization failed. <Reason initialization failed>. <Internal error code>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that trace was unable to initialize.

Recommended Action

Execute the `supportSave` command and reload the switch. If the problem persists, contact your switch service provider.

KTRC-1006

Message

Trace corruption found. <Trace corruption status>. <Trace corruption error code>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that trace corruption was found.

Recommended Action

Execute the `supportSave` command and reload the switch. If the problem persists, contact your switch service provider.

LACP Messages

LACP module error messages.

LACP-1001

Message

<module> Error opening socket (<error>).

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that initialization of the specified module within the Link Aggregation Control Protocol (LACP) daemon has failed.

Recommended Action

Download a new firmware using the `firmwareDownload` command.

LACP-1002

Message

<msg>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that some of the fields received in the Link Aggregation Control Protocol Data Unit (LACPDU) are invalid.

LACP-1003

Message

<msg>.

Message Type

LOG | FFDC

Message Severity

WARNING

Probable Cause

Indicate port state expired.

LFM Messages

Logical Fabric Manager module error messages.

LFM-1001

Message

The Logical Fabric Manager service is disabled.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the Logical Fabric Manager service is disabled. Note that the Logical Fabric Manager service is enabled by the factory setting and it is not user-configurable.

LFM-1002

Message

The Logical Fabric Manager service is enabled.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the Logical Fabric Manager service is enabled. Note that the Logical Fabric Manager service is enabled by the factory setting and it is not user-configurable.

LFM-1003

Message

The Logical Fabric Manager configuration is set to default.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the Logical Fabric Manager configuration is set to default. This will remove all prior Logical Fabric Manager configurations. This operation is not supported currently.

LFM-1004**Message**

HA is out of sync for opcode <HA OPCODE>, error value <error value>.

Message Type

LOG | FFDC

Message Severity

CRITICAL

Probable Cause

Indicates loss of high availability (HA) sync with remote control processor (CP).

Recommended Action

Collect the supportsave information using the `supportsave` command and contact the Brocade technical support.

LFM-1005**Message**

Logical port <portnum> disabled with reason <reason code>(<reason string>)

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the specified logical port is disabled for an internal logging purpose. This could be due to port segmentation.

Recommended Action

Check the reason for port disable using the `switchShow` command, and take appropriate corrective action.

LFM-1006

Message

The switch with domain <domain> with firmware version <version> has joined the FID <FID> fabric and may not be compatible with XISL use.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the firmware version on the specified switch is not compatible with XISL.

Recommended Action

Check the release notes to verify if this firmware is compatible with XISL. If it is not, remove the switch from the fabric.

LFM-1007

Message

Logical ISLs are enabled for FID <FID>.

Message Type

AUDIT | LOG

Message Class

LS

Message Severity

INFO

Probable Cause

Indicates that Logical ISLs are enabled for specified logical fabric.

LIC Messages

License module error messages.

LIC-1000

Message

Blade slot <slot number> added to <license feature name> slot-based license configuration.

Message Type

AUDIT | LOG

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates a slot has been configured to allow a specific license feature.

LIC-1001

Message

Blade slot <slot number> removed from <license feature name> slot-based license configuration.

Message Type

AUDIT | LOG

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates a slot has been removed from a specific license feature configuration.

LIC-1002

Message

License log file is corrupted. Exceeded 10 warning limit within the monitoring period. All login sessions will be blocked.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the CLP log file was deleted or changed by the user.

Recommended Action

Check date and time on /var/log/clp_license.log.

LIC-1003**Message**

license install failed 25 times within the monitoring period.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that there were 25 license install failures in 24 hours.

Recommended Action

Do not add any more invalid license keys.

LIC-1004**Message**

license install failed 40 times within the monitoring period. All login sessions will be blocked after 10 more failures

Message Type

LOG

Message Severity

CRITICAL

Probable Cause

Indicates that there were 40 license install failures in 24 hours.

Recommended Action

>Do not add any more invalid license keys.

LIC-1005**Message**

license install failed 50 times within the monitoring period. All login sessions will be blocked

Message Type

LOG

Message Severity

CRITICAL

Probable Cause

Indicates that there were 50 license install failures in 24 hours.

Recommended Action

>User will need to contact Broadcom BSN TAC to recover.

LIC-1009**Message**

License system integrity check failed, license operations are blocked.

Message Type

LOG

Message Severity

CRITICAL

Probable Cause

Indicates that license public key hash check has failed.

Recommended Action

Contact the customer support and get the license seeprom programmed.

LIC-1010**Message**

<Key> license has expired.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates the license period has expired.

Recommended Action

Get a new license for this feature.

LIC-2000**Message**

Accept Brocade FOS End User License Agreement.

Message Type

AUDIT

Message Class

FIRMWARE

Message Severity

INFO

Probable Cause

Indicates user accept Brocade FOS End User License Agreement at the first login into a Factory shipped system.

Recommended Action

>No action is required.

LIC-2001**Message**

Fail to accept Brocade FOS End User License Agreement.

Message Type

AUDIT

Message Class

FIRMWARE

Message Severity

INFO

Probable Cause

Indicates user fail to accept Brocade FOS End User License Agreement at the first login into a Factory shipped system.

Recommended Action

Relogin and accept Brocade FOS End User License Agreement.

LIC-2002

Message

<ras_msg>

Message Type

AUDIT

Message Class

CFG

Message Severity

ERROR

Probable Cause

LIC-2003

Message

<ras_msg>

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

LOG Messages

RASLog subsystem messages.

LOG-1000

Message

Previous message repeated <repeat count> time(s).

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the previous message was repeated the specified number of times.

LOG-1001**Message**

A log message was dropped.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that a log message was dropped. A trace dump file has been created.

Recommended Action

Execute the `reboot` command for non-bladed switches or the `haFailover` command on bladed switches.

If the message persists, execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

LOG-1002**Message**

A log message was dropped.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that a message was not recorded by the error logging system. A trace dump file has been created. The message may still be visible through Simple Network Management Protocol (SNMP) or other management tools.

Recommended Action

Execute the `reboot` command for non-bladed switches or the `haFailover` command on bladed switches.

If the message persists, execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

LOG-1003

Message

The log has been cleared.

Message Type

AUDIT | LOG

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the persistent error log has been cleared.

LOG-1004

Message

Log message <Log message that has been blocked> flooding detected and blocked.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that a message has been flooding and was blocked.

Recommended Action

If the message persists, execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

LOG-1005

Message

Log message <Log message that has been disabled> has been disabled.

Message Type

AUDIT | LOG

Message Class

RAS

Message Severity

INFO

Probable Cause

Indicates that the specified message has been disabled from logging.

LOG-1006

Message

Log message <Log message that has been enabled> has been enabled.

Message Type

AUDIT | LOG

Message Class

RAS

Message Severity

INFO

Probable Cause

Indicates that the specified message has been enabled for logging.

LOG-1007

Message

Log Module <Log Module that has been disabled> has been disabled.

Message Type

AUDIT | LOG

Message Class

RAS

Message Severity

INFO

Probable Cause

Indicates that the specified module has been disabled from logging.

LOG-1008**Message**

Log Module <Log Module that has been enabled> has been enabled.

Message Type

AUDIT | LOG

Message Class

RAS

Message Severity

INFO

Probable Cause

Indicates that the specified module has been enabled for logging.

LOG-1009**Message**

Internal Log message <Log message that has been enabled to be sent to syslog server> has been enabled for syslog logging.

Message Type

AUDIT | LOG

Message Class

RAS

Message Severity

INFO

Probable Cause

Indicates that the specified internal message has been enabled for syslog logging.

LOG-1010

Message

Internal Log message <Log message that has been disabled from being sent to syslog server> has been disabled from syslog logging.

Message Type

AUDIT | LOG

Message Class

RAS

Message Severity

INFO

Probable Cause

Indicates that the specified internal message has been disabled from syslog logging.

LOG-1011

Message

Log Message <Log Message Id> severity has been changed to <Severity>.

Message Type

AUDIT | LOG

Message Class

RAS

Message Severity

INFO

Probable Cause

Indicates that the severity level of the specified log message has been changed.

LOG-1012

Message

Ras Quiet Time is enabled for <String>.

Message Type

AUDIT | LOG

Message Class

RAS

Message Severity

INFO

Probable Cause

Indicates that quiet time is enabled.

LOG-1013

Message

Ras Quiet Time is disabled for <String>.

Message Type

AUDIT | LOG

Message Class

RAS

Message Severity

INFO

Probable Cause

Indicates that quiet time is disabled.

LSDB Messages

Link state database error messages.

LSDB-1001

Message

Link State ID <link state ID> out of range.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the specified link state ID is out of the acceptable range. The valid link state ID is the same as the valid domain ID, with a range from 1 through 239. The switch will discard the record because it is not supported.

LSDB-1002**Message**

Local Link State Record reached max incarnation.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the local link state record (LSR) reached the maximum number of incarnations.

An "incarnation" is a progressive number that identifies the most recent version of the link state record (LSR). The switch generates its local LSR when first enabled. The incarnation number will begin again at 0x80000001 after reaching 0x7FFFFFFF.

LSDB-1003**Message**

No database entry for local Link State Record, domain <local domain>.

Message Type

FFDC | LOG

Message Severity

CRITICAL

Probable Cause

Indicates that there is no local link state record (LSR) entry in the link state database (LSDB). The switch should always generate its own local entry when starting up.

An "incarnation" is a progressive number that identifies the most recent version of the LSR. The switch generates its local LSR when first enabled. By disabling and enabling the switch, a new local LSR is generated.

Recommended Action

Run the `switchDisable` and `switchEnable` commands. A new local LSR is generated during the switch enable.

LSDB-1004

Message

No Link State Record for domain <local domain>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that there is no link state record (LSR) for the specified local domain.

Recommended Action

No action is required. The other switch will pass the LSR after the fabric is stable.

LSDB-1005

Message

HA out of sync due to FSPF DB size larger than standby CP supports.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the maximum link state database (LSDB) size supported by the standby control processor (CP) is less than that of the active CP.

Recommended Action

Upgrade the standby firmware to active CP firmware version.

MAPS Messages

MAPS module error messages.

MAPS-1001 to MAPS-1004

Message

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>, Quiet Time=<Quiet Time>.

Message Type

LOG

Message Severity

['MAPS-1001 : CRITICAL', 'MAPS-1002 : ERROR', 'MAPS-1003 : WARNING', 'MAPS-1004 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-1005

Message

<object>, Condition=<condition>, Current Value:<ms, values, units>, Rule <Rule name> triggered <count> times in <QT> and last trigger time <execution time>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-1006

Message

<object>, Latest <value or state>=<Latest value or state of MS(ms, value, units)>.

Message Type

LOG

Message Severity

INFO

Probable Cause

This is a support information to MAPS-1005 and it is triggered to display the latest value of MS that is triggered as part of MAPS-1005.

MAPS-1010**Message**

Port(s) fenced due to RuleName=<Rule name>, Condition=<condition>, Obj:<object> <ms, values, units>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold, and therefore the specified ports are fenced.

Recommended Action

Respond to this message as is appropriate to the particular policy of the end-user installation.

MAPS-1011**Message**

Port(s) decommissioned due to RuleName=<Rule name>, Condition=<condition>, Obj:<object> <ms, values, units>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold, and therefore the specified ports are fenced.

Recommended Action

Respond to this message as is appropriate to the particular policy of the end-user installation.

MAPS-1012

Message

Port decommission action failed on port <object>, with reason string, <reason>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the port decommission has failed on an object.

Recommended Action

Respond to this message as is appropriate to the particular policy of the end-user installation.

MAPS-1013

Message

Port(s) impaired due to RuleName=<Rule name>, Condition=<condition>, Obj:<object> <ms, values, units>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold, and therefore the specified ports are impaired.

Recommended Action

Respond to this message as is appropriate to the particular policy of the end-user installation.

MAPS-1014

Message

Port impair action failed on port <object>, with reason string, <reason>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the port impair action has failed on an object.

Recommended Action

Respond to this message as is appropriate to the particular policy of the end-user installation.

MAPS-1015

Message

MAPS recipient email address list got updated.

Message Type

LOG | AUDIT

Message Class

MAPS

Message Severity

INFO

Probable Cause

Indicates MAPS email address configuration is set to given email address or list which would be used as recipient email address for EMAIL notifications.

MAPS-1016

Message

MAPS originator email address got updated.

Message Type

LOG | AUDIT

Message Class

MAPS

Message Severity

INFO

Probable Cause

Indicates MAPS email address configuration is set to given email address which would be used as originator email address for EMAIL notifications.

MAPS-1017**Message**

MAPS relayConfig got updated to relay_IP: <relay_IP>, domain: <domain>.

Message Type

LOG | AUDIT

Message Class

MAPS

Message Severity

INFO

Probable Cause

Relay IP and Domain Name configuration change.

MAPS-1018**Message**

MAPS decommission action config set to mode <decom config>.

Message Type

LOG | AUDIT

Message Class

MAPS

Message Severity

INFO

Probable Cause

Decommission mode configuration change.

MAPS-1020**Message**

Switch wide status has changed from <Previous state> to <Current state>.

Message Type

LOG | AUDIT

Message Class

MAPS

Message Severity

WARNING

Probable Cause

Indicates a change in the state of the switch. This log provides the previous state and the current state of the switch.

Recommended Action

Check the accompanying RASLog messages to determine the cause of the state change.

MAPS-1021**Message**

RuleName=<Rule name>, Condition=<condition>, Obj:<object, units> <Old state> has contributed to switch status <New state>.

Message Type

LOG | AUDIT

Message Class

MAPS

Message Severity

WARNING

Probable Cause

Indicates the specified rule has been violated and as a consequence has contributed to the mentioned state of the switch.

MAPS-1022**Message**

Port <slotport> (Port index <portindex>) has been marked as Slow Drain Device.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the quarantine action for the port due to Severe Latency / Frame Loss has been initiated. Traffic destined to this port will be moved to low QoS Virtual Channel at source.

MAPS-1023**Message**

Port <slotport> marked as Slow Drain Device is not enforced due to zoned port limit exceeded.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the port flagged for Severe Latency / Frame Loss could not be quarantined due to the zoned port count more than 32.

Recommended Action

Requires manual intervention to set the slow drain condition right.

MAPS-1024**Message**

Configured limit exceeded. Port <slotport> could not be marked as Slow Drain Device.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the port flagged for Severe Latency / Frame Loss could not be quarantined, since the configured limit was exceeded.

Recommended Action

Requires manual intervention to set the slow drain condition right or the limit has to be reconfigured.

MAPS-1025

Message

Port <slotport> (Port index <portindex>) removed from the Slow Drain Device Quarantine Group.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the port flagged for Severe Latency / Frame Loss earlier has been removed from the quarantine group.

MAPS-1026

Message

MAPS aborted port un-quarantine action for port(s) <slotport>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that there is configdownload or new policy enabled.

Recommended Action

Manually un-quarantine ports using `sddquarantine --clear` command.

MAPS-1027

Message

Device login state rebalanced for FI <nodewwn>.

Message Type

AUDIT

Message Class

MAPS

Message Severity

WARNING

Probable Cause

Indicates that the Cisco devices through FI have been un-equally loaded among all ports connected to FI.

Recommended Action

Manually balances ports connected to FI cisco devices by using devicelogin --rebalance command.

MAPS-1028

Message

Clearing quarantined state of ports.

Message Type

AUDIT

Message Class

MAPS

Message Severity

INFO

Probable Cause

Indicates quarantined state of ports got cleared.

Recommended Action

Manually quarantined state of ports gets cleared by using sddquarantine --clear command.

MAPS-1100

Message

Rule <Rule name> is created.

Message Type

LOG | AUDIT

Message Class

MAPS

Message Severity

INFO

Probable Cause

Indicates that the specified rule was created in the system.

Recommended Action

Make sure the configuration change is expected.

MAPS-1101**Message**

Rule <Rule name> is deleted.

Message Type

LOG | AUDIT

Message Class

MAPS

Message Severity

INFO

Probable Cause

Indicates that the specified rule was deleted from the system.

Recommended Action

Make sure the configuration change is expected.

MAPS-1102**Message**

Rule <Rule name> is modified.

Message Type

LOG | AUDIT

Message Class

MAPS

Message Severity

INFO

Probable Cause

Indicates that the specified rule was modified in the system.

Recommended Action

Make sure the configuration change is expected.

MAPS-1110**Message**

Policy <Policy name> is created.

Message Type

LOG | AUDIT

Message Class

MAPS

Message Severity

INFO

Probable Cause

Indicates that the specified policy was created in the system.

Recommended Action

Make sure the configuration change is expected.

MAPS-1111**Message**

Policy <Policy name> is deleted.

Message Type

LOG | AUDIT

Message Class

MAPS

Message Severity

INFO

Probable Cause

Indicates that the specified policy was deleted from the system.

Recommended Action

Make sure the configuration change is expected.

MAPS-1112

Message

Policy <Source Policy name> cloned to <Target Policy name>.

Message Type

LOG | AUDIT

Message Class

MAPS

Message Severity

INFO

Probable Cause

Indicates that the specified policy was cloned in the system.

Recommended Action

Make sure the configuration change is expected.

MAPS-1113

Message

Policy <Policy name> activated.

Message Type

LOG | AUDIT

Message Class

MAPS

Message Severity

INFO

Probable Cause

Indicates that the specified policy was activated in the system.

Recommended Action

Make sure the configuration change is expected.

MAPS-1114

Message

Rule <Rule name> added to Policy <Policy name>.

Message Type

LOG | AUDIT

Message Class

MAPS

Message Severity

INFO

Probable Cause

Indicates that the specified rule was added to the specified policy.

Recommended Action

Make sure the configuration change is expected.

MAPS-1115

Message

Rule <Rule name> deleted from Policy <Policy name>.

Message Type

LOG | AUDIT

Message Class

MAPS

Message Severity

INFO

Probable Cause

Indicates that the specified rule was deleted from the specified policy.

Recommended Action

Make sure the configuration change is expected.

MAPS-1116

Message

Policy <Policy name> updated.

Message Type

LOG | AUDIT

Message Class

MAPS

Message Severity

INFO

Probable Cause

Indicates that the specified policy was updated.

Recommended Action

Make sure the configuration change is expected.

MAPS-1120

Message

Group <Group name> created.

Message Type

LOG | AUDIT

Message Class

MAPS

Message Severity

INFO

Probable Cause

Indicates that the specified group was created.

Recommended Action

Make sure the configuration change is expected.

MAPS-1121

Message

Group <Group name> deleted.

Message Type

LOG | AUDIT

Message Class

MAPS

Message Severity

INFO

Probable Cause

Indicates that the specified group was deleted.

Recommended Action

Make sure the configuration change is expected.

MAPS-1122

Message

Group <Source group name> cloned to <Target group name>.

Message Type

LOG | AUDIT

Message Class

MAPS

Message Severity

INFO

Probable Cause

Indicates that the specified group was cloned.

Recommended Action

Make sure the configuration change is expected.

MAPS-1123

Message

Group <Group name> modified.

Message Type

LOG | AUDIT

Message Class

MAPS

Message Severity

INFO

Probable Cause

Indicates that the specified group was modified.

Recommended Action

Make sure the configuration change is expected.

MAPS-1124

Message

Flow <Flow name> imported.

Message Type

LOG | AUDIT

Message Class

MAPS

Message Severity

INFO

Probable Cause

Indicates that the specified flow from Flow Vision is imported into MAPS.

Recommended Action

Make sure the configuration change is expected.

MAPS-1125

Message

Flow <Flow name> deimported.

Message Type

LOG | AUDIT

Message Class

MAPS

Message Severity

INFO

Probable Cause

Indicates that the specified flow was removed from MAPS.

Recommended Action

Make sure the configuration change is expected.

MAPS-1126

Message

Imported flow <Flow name> is a stale flow or currently does not exist in flow vision.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the specified flow does not exist in Flow Vision.

Recommended Action

Make sure the configuration change is expected.

MAPS-1127

Message

Imported flow <Flow name> is initialized as stale flow because it is <Flow description>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that MAPS has imported the specified flow present in the configuration and initialized it as stale flow due to the mentioned reason.

Recommended Action

Make sure the configuration change is expected.

MAPS-1130**Message**

Actions <List of actions configured> configured.

Message Type

LOG | AUDIT

Message Class

MAPS

Message Severity

INFO

Probable Cause

Indicates that the specified list of actions are configured.

Recommended Action

Make sure the configuration change is expected.

MAPS-1131**Message**

Monitoring on members <List of members/objects > of type <Type of members/objects> is paused.

Message Type

LOG | AUDIT

Message Class

MAPS

Message Severity

INFO

Probable Cause

Indicates that monitoring on the specified list of members is paused.

Recommended Action

Make sure the configuration change is expected.

MAPS-1132**Message**

Monitoring on members <List of members/objects > of type <Type of members/objects> is restarted.

Message Type

LOG | AUDIT

Message Class

MAPS

Message Severity

INFO

Probable Cause

Indicates that monitoring on the specified list of members has resumed.

Recommended Action

Make sure the configuration change is expected.

MAPS-1133**Message**

Rules were cloned from existing group <source group name> to new policy <new policy name> successfully.

Message Type

LOG | AUDIT

Message Class

MAPS

Message Severity

INFO

Probable Cause

Indicates that the rules were cloned from src group to new policy.

Recommended Action

Make sure the configuration change is expected.

MAPS-1134

Message

The profile <profile name> changed threshold <old threshold value> to <new threshold value>, description [<old description value>] to [<new description value>].

Message Type

LOG | AUDIT

Message Class

MAPS

Message Severity

INFO

Probable Cause

Indicates the profile threshold and(or) description is updated successfully.

MAPS-1135

Message

Initiated flow profile activation.

Message Type

LOG | AUDIT

Message Class

MAPS

Message Severity

INFO

Probable Cause

Indicates Flow Profiles are activated successfully.

MAPS-1136**Message**

Flow Profiles are cleared.

Message Type

LOG | AUDIT

Message Class

MAPS

Message Severity

INFO

Probable Cause

Indicates Flow Profiles are cleared successfully.

MAPS-1137**Message**

All the Profile configuration data is reset to default values and Flow Profile are activated.

Message Type

LOG | AUDIT

Message Class

MAPS

Message Severity

INFO

Probable Cause

Indicates all the profile configuration data is reset to default values.

MAPS-1138**Message**

Flow profiles activation is successful.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates profiles activation is successful.

MAPS-1139**Message**

Flow profiles activation is failed.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates profiles activation is successful.

MAPS-1140**Message**

FPI Profile < FPI Profile name > is created.

Message Type

LOG | AUDIT

Message Class

MAPS

Message Severity

INFO

Probable Cause

Indicates that new FPI Profile is created with custom thresholds

Recommended Action

Make sure the configuration change is expected.

MAPS-1141

Message

FPI Profile < FPI Profile name > is deleted.

Message Type

LOG | AUDIT

Message Class

MAPS

Message Severity

INFO

Probable Cause

Indicates that new FPI Profile is deleted

Recommended Action

Make sure the configuration change is expected.

MAPS-1142

Message

FPI Profile < Source FPI Profile name > is cloned to < Target FPI Profile name >.

Message Type

LOG | AUDIT

Message Class

MAPS

Message Severity

INFO

Probable Cause

Indicates that new FPI Profile is cloned from existing profile

Recommended Action

Make sure the configuration change is expected.

MAPS-1143

Message

FPI Profile <FPI Profile name > is modified.

Message Type

LOG | AUDIT

Message Class

MAPS

Message Severity

INFO

Probable Cause

Indicates that FPI Profile threshold(s) modified

Recommended Action

Make sure the configuration change is expected.

MAPS-1144

Message

FPI Profile < FPI Profile name > is activated for F-Ports.

Message Type

LOG | AUDIT

Message Class

MAPS

Message Severity

INFO

Probable Cause

Indicates that new FPI thresholds is activated

MAPS-1145

Message

FPI Profile < FPI Profile name > is activated for E-Ports.

Message Type

LOG | AUDIT

Message Class

MAPS

Message Severity

INFO

Probable Cause

Indicates that new FPI thresholds is activated

MAPS-1146

Message

Time changed on switch re-starting MAPS monitoring.

Message Type

LOG | AUDIT

Message Class

MAPS

Message Severity

INFO

Probable Cause

Indicates switch time changed so MAPS monitoring has to be aligned to new switch time.

Recommended Action

Previous MAPS dashboard data will indicate old switch time. Issue a mapsdb --clear if required.

MAPS-1147

Message

Certificate <certificate name> of type <certificate type> with date <certificate date> beyond year 2038 is not monitored.

Message Type

LOG | AUDIT

Message Class

MAPS

Message Severity

WARNING

Probable Cause

Indicates that calendar date is beyond 2038 and it hits Y2K2038 problem where time data type overflows.

Recommended Action

Input the calendar date within 2038.

MAPS-1148**Message**

No Flow Vision license, changing active policy to < base policy > from < configured policy >.

Message Type

LOG | AUDIT

Message Class

MAPS

Message Severity

INFO

Probable Cause

License expired or deleted from switch

Recommended Action

Install Flow Vision license for complete MAPS functionality.

MAPS-1199**Message**

MAPS has encountered a critical issue with reason <reason>.

Message Type

LOG | AUDIT | FFDC

Message Class

MAPS

Message Severity

CRITICAL

Probable Cause

Critical issue has happened

Recommended Action

Customer needs to do HA failover for chassis or HA reboot for pizza box system immediatly.

MAPS-1200**Message**

MAPS rules have used all the hardware profiles to monitor latency -
RD_STATUS_TIME,WR_STATUS_TIME,RD_1stDATA_TIME,WR_1stXFER_RDY.

Message Type

LOG

Message Severity

ERROR

Probable Cause**Recommended Action**

User can mitigate this issue as follows: a. Checkout rules to monitor
RD_STATUS_TIME,WR_STATUS_TIME,RD_1stDATA_TIME,WR_1stXFER_RDY with timebase IO in each logical switch.
b. If some rules are not needed then please delete the rules. c. Reactivate the policy.

MAPS-1201**Message**

MAPS has started monitoring with <Policy name> policy.

Message Type

LOG | AUDIT

Message Class

MAPS

Message Severity

INFO

Probable Cause

Indicates that MAPS has started monitoring the system

Recommended Action

Make sure the configuration change is expected.

MAPS-1202**Message**

MAPS policy <policy name> is not present. Re-enable MAPS with different policy.

Message Type

LOG | AUDIT

Message Class

MAPS

Message Severity

INFO

Probable Cause

Indicates that MAPS policy is not available in the system. Re-enable MAPS with a different policy.

Recommended Action

Make sure the configuration change is expected.

MAPS-1203**Message**

Dashboard <data type> data has been cleared.

Message Type

LOG | AUDIT

Message Class

MAPS

Message Severity

WARNING

Probable Cause

Indicates that the dashboard has been cleared.

MAPS-1204

Message

MAPS aborted port toggle action on port <port>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that port toggle state has been changed.

MAPS-1205

Message

Port toggle action is successful on port <port>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that port toggle action is successful.

MAPS-1206

Message

A MAPS email notification sent from the switch could not be delivered to Email server.

Message Type

LOG | AUDIT

Message Class

MAPS

Message Severity

INFO

Probable Cause

Indicates that an e-mail from the switch to the address has failed.

Recommended Action

The problem needs to be debugged.

MAPS-1207**Message**

There were <Number of email delivery errors> email delivery errors in the last hour.

Message Type

LOG | AUDIT

Message Class

MAPS

Message Severity

INFO

Probable Cause

Indicates that some e-mails from the switch encountered errors.

Recommended Action

The problem needs to be debugged.

MAPS-1208**Message**

Raslog mode is set to <mode>.

Message Type

LOG | AUDIT

Message Class

MAPS

Message Severity

INFO

Probable Cause

raslog mode has been changed

Recommended Action**MAPS-1209****Message**

Global Quiet Time enabled with <Global Quiet Time Value>.

Message Type

LOG | AUDIT

Message Class

MAPS

Message Severity

INFO

Probable Cause

Global Quiet Time enabled

Recommended Action**MAPS-1210****Message**

Global Quiet Time disabled.

Message Type

LOG | AUDIT

Message Class

MAPS

Message Severity

INFO

Probable Cause

Global Quiet Time disabled

Recommended Action

MAPS-1211

Message

Monitoring is paused for members of group type <List of group types which has paused members>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Paused Members

Recommended Action

MAPS-1213

Message

Monitoring is paused for all the supported group-types.

Message Type

LOG

Message Severity

INFO

Probable Cause

Monitoring is paused for all the supported group-types

Recommended Action

MAPS-1214

Message

Monitoring restarted for all the supported group-types.

Message Type

LOG

Message Severity

INFO

Probable Cause

Monitoring is restarted for all the supported group-types

Recommended Action

MAPS-1215

Message

Monitoring is paused for the specified group type (<Group Type>).

Message Type

LOG

Message Severity

INFO

Probable Cause

Monitoring is paused for the specified group type

Recommended Action

MAPS-1216

Message

Monitoring restarted for the specified group type (<Group Type>).

Message Type

LOG

Message Severity

INFO

Probable Cause

Monitoring is restarted for the specified group type

Recommended Action

MAPS-1217

Message

Duplicate rules have been found to monitor
RD_STATUS_TIME,WR_STATUS_TIME,RD_1stDATA_TIME,WR_1stXFER_RDY. Rule Name = <rule Name>

Message Type

LOG

Message Severity

ERROR

Probable Cause

Recommended Action

User can mitigate this issue as follows: a. Checkout rules to monitor
RD_STATUS_TIME,WR_STATUS_TIME,RD_1stDATA_TIME,WR_1stXFER_RDY with timebase IO in the logical switch.
b. Delete the duplicate rules. c. Reactivate the policy.

MAPS-1220

Message

MAPS Notification mode is set to <>.

Message Type

LOG | AUDIT

Message Class

MAPS

Message Severity

INFO

Probable Cause

MAPS Notification behaviour is changed

Recommended Action

MAPS-1301

Message

Application server <server> is bound with the logical partition.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that application server bind operation is successful.

MAPS-1302

Message

Application server <server> is unbound with the logical partition.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that application server unbind operation is successful.

MAPS-2000

Message

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

CRITICAL

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2001

Message

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2002

Message

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2003

Message

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2004 to MAPS-2007**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>, Quiet Time=<Quiet Time>.

Message Type

LOG

Message Severity

['MAPS-2004 : CRITICAL', 'MAPS-2005 : ERROR', 'MAPS-2006 : WARNING', 'MAPS-2007 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

Recommended Action

Check your small form-factor pluggable (SFPs), cables, and connections on local and remote side.

MAPS-2008 to MAPS-2011**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>, Quiet Time=<Quiet Time>.

Message Type

LOG

Message Severity

['MAPS-2008 : CRITICAL', 'MAPS-2009 : ERROR', 'MAPS-2010 : WARNING', 'MAPS-2011 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

Recommended Action

Check your small form-factor pluggable (SFPs), cables, and connections on local and remote side.

MAPS-2012 to MAPS-2015

Message

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>, Quiet Time=<Quiet Time>.

Message Type

LOG

Message Severity

['MAPS-2012 : CRITICAL', 'MAPS-2013 : ERROR', 'MAPS-2014 : WARNING', 'MAPS-2015 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

Recommended Action

Check your small form-factor pluggable (SFPs), cables, and connections on local and remote side.

MAPS-2016 to MAPS-2019

Message

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>, Quiet Time=<Quiet Time>.

Message Type

LOG

Message Severity

['MAPS-2016 : CRITICAL', 'MAPS-2017 : ERROR', 'MAPS-2018 : WARNING', 'MAPS-2019 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

Recommended Action

Check your small form-factor pluggable (SFPs), cables, and connections on local and remote side.

MAPS-2020 to MAPS-2023

Message

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>, Quiet Time=<Quiet Time>.

Message Type

LOG

Message Severity

['MAPS-2020 : CRITICAL', 'MAPS-2021 : ERROR', 'MAPS-2022 : WARNING', 'MAPS-2023 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

Recommended Action

Check your small form-factor pluggable (SFPs), cables, and connections on local and remote side.

MAPS-2024 to MAPS-2027**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>, Quiet Time=<Quiet Time>.

Message Type

LOG

Message Severity

['MAPS-2024 : CRITICAL', 'MAPS-2025 : ERROR', 'MAPS-2026 : WARNING', 'MAPS-2027 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

Recommended Action

Check your small form-factor pluggable (SFPs), cables, and connections on local and remote side.

MAPS-2028 to MAPS-2031**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>, Quiet Time=<Quiet Time>.

Message Type

LOG

Message Severity

['MAPS-2028 : CRITICAL', 'MAPS-2029 : ERROR', 'MAPS-2030 : WARNING', 'MAPS-2031 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

Recommended Action

The state of the port has changed for one of the following reasons: the port has gone offline, has come online, is faulty. If the change is not an expected event in the environment, then it is most likely due to physical errors. In that case, check both sides of the cable, SFPs and make sure they are not faulty.

MAPS-2032 to MAPS-2035**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>, Quiet Time=<Quiet Time>.

Message Type

LOG

Message Severity

['MAPS-2032 : CRITICAL', 'MAPS-2033 : ERROR', 'MAPS-2034 : WARNING', 'MAPS-2035 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

Recommended Action

Check your small form-factor pluggable (SFPs), cables, and connections on local and remote side.

MAPS-2036 to MAPS-2039**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>, Quiet Time=<Quiet Time>.

Message Type

LOG

Message Severity

['MAPS-2036 : CRITICAL', 'MAPS-2037 : ERROR', 'MAPS-2038 : WARNING', 'MAPS-2039 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

Recommended Action

Check the target device; it could be operating at sub-optimal speed to receive frames.

MAPS-2040 to MAPS-2043

Message

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>, Quiet Time=<Quiet Time>.

Message Type

LOG

Message Severity

['MAPS-2040 : CRITICAL', 'MAPS-2041 : ERROR', 'MAPS-2042 : WARNING', 'MAPS-2043 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

Recommended Action

High utilization may indicate a need for more bandwidth or redistributing traffic (load balancing).

MAPS-2044 to MAPS-2047

Message

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>, Quiet Time=<Quiet Time>.

Message Type

LOG

Message Severity

['MAPS-2044 : CRITICAL', 'MAPS-2045 : ERROR', 'MAPS-2046 : WARNING', 'MAPS-2047 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

Recommended Action

High utilization may indicate a need for more bandwidth or redistributing traffic (load balancing).

MAPS-2048 to MAPS-2051

Message

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>, Quiet Time=<Quiet Time>.

Message Type

LOG

Message Severity

['MAPS-2048 : CRITICAL', 'MAPS-2049 : ERROR', 'MAPS-2050 : WARNING', 'MAPS-2051 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

Recommended Action

High utilization may indicate a need for more bandwidth or redistributing traffic (load balancing).

MAPS-2052 to MAPS-2055

Message

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

['MAPS-2052 : CRITICAL', 'MAPS-2053 : ERROR', 'MAPS-2054 : WARNING', 'MAPS-2055 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2056 to MAPS-2059

Message

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

['MAPS-2056 : CRITICAL', 'MAPS-2057 : ERROR', 'MAPS-2058 : WARNING', 'MAPS-2059 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2060 to MAPS-2063

Message

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>, Quiet Time=<Quiet Time>.

Message Type

LOG

Message Severity

['MAPS-2060 : CRITICAL', 'MAPS-2061 : ERROR', 'MAPS-2062 : WARNING', 'MAPS-2063 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

Recommended Action

Check your small form-factor pluggable (SFPs), cables, and connections on local and remote side.

MAPS-2064 to MAPS-2067

Message

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>, Quiet Time=<Quiet Time>.

Message Type

LOG

Message Severity

['MAPS-2064 : CRITICAL', 'MAPS-2065 : ERROR', 'MAPS-2066 : WARNING', 'MAPS-2067 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

Recommended Action

Check your small form-factor pluggable (SFPs), cables, and connections on local and remote side

MAPS-2068 to MAPS-2071

Message

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>, Quiet Time=<Quiet Time>.

Message Type

LOG

Message Severity

['MAPS-2068 : CRITICAL', 'MAPS-2069 : ERROR', 'MAPS-2070 : WARNING', 'MAPS-2071 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

Recommended Action

Isolate the devices causing the latency impact and disable the impacted switch ports.

MAPS-2072 to MAPS-2075

Message

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

['MAPS-2072 : CRITICAL', 'MAPS-2073 : ERROR', 'MAPS-2074 : WARNING', 'MAPS-2075 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2076 to MAPS-2079

Message

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

['MAPS-2076 : CRITICAL', 'MAPS-2077 : ERROR', 'MAPS-2078 : WARNING', 'MAPS-2079 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2080 to MAPS-2083

Message

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>, Quiet Time=<Quiet Time>.

Message Type

LOG

Message Severity

['MAPS-2080 : CRITICAL', 'MAPS-2081 : ERROR', 'MAPS-2082 : WARNING', 'MAPS-2083 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

Recommended Action

Reduce the number of NPIV logins to the port as per the configured limit to avoid unnecessary logins from devices and usage of resources.

MAPS-2084 to MAPS-2087

Message

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

['MAPS-2084 : CRITICAL', 'MAPS-2085 : ERROR', 'MAPS-2086 : WARNING', 'MAPS-2087 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2088 to MAPS-2091

Message

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>, Quiet Time=<Quiet Time>.

Message Type

LOG

Message Severity

['MAPS-2088 : CRITICAL', 'MAPS-2089 : ERROR', 'MAPS-2090 : WARNING', 'MAPS-2091 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

Recommended Action

AMP reached the maximum IOs throughput capability. Consider using multiple AMPs and distribute the flows from the fabric among them. Refer to admin guide for further assistance on the procedure.

MAPS-2092 to MAPS-2095**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>, Quiet Time=<Quiet Time>.

Message Type

LOG

Message Severity

['MAPS-2092 : CRITICAL', 'MAPS-2093 : ERROR', 'MAPS-2094 : WARNING', 'MAPS-2095 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

Recommended Action

Reboot the switch or reboot the blade.

MAPS-2096 to MAPS-2099**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>, Quiet Time=<Quiet Time>.

Message Type

LOG

Message Severity

['MAPS-2096 : CRITICAL', 'MAPS-2097 : ERROR', 'MAPS-2098 : WARNING', 'MAPS-2099 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

Recommended Action

Reboot the switch or reboot the blade.

MAPS-2100 to MAPS-2103**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>, Quiet Time=<Quiet Time>.

Message Type

LOG

Message Severity

['MAPS-2100 : CRITICAL', 'MAPS-2101 : ERROR', 'MAPS-2102 : WARNING', 'MAPS-2103 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

Recommended Action

Reboot the switch or reboot the blade.

MAPS-2104 to MAPS-2107**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>, Quiet Time=<Quiet Time>.

Message Type

LOG

Message Severity

['MAPS-2104 : CRITICAL', 'MAPS-2105 : ERROR', 'MAPS-2106 : WARNING', 'MAPS-2107 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

Recommended Action

AMP reached the maximum IOs throughput capability. Consider using multiple AMPs and distribute the flows from the fabric among them. Refer to admin guide for further assistance on the procedure.

MAPS-2108 to MAPS-2111

Message

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>, Quiet Time=<Quiet Time>.

Message Type

LOG

Message Severity

['MAPS-2108 : CRITICAL', 'MAPS-2109 : ERROR', 'MAPS-2110 : WARNING', 'MAPS-2111 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

Recommended Action

Reseat the blade or reboot the switch.

MAPS-2112 to MAPS-2115

Message

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>, Quiet Time=<Quiet Time>.

Message Type

LOG

Message Severity

['MAPS-2112 : CRITICAL', 'MAPS-2113 : ERROR', 'MAPS-2114 : WARNING', 'MAPS-2115 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

Recommended Action

Reseat the blade or reboot the switch.

MAPS-2116 to MAPS-2119

Message

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>, Quiet Time=<Quiet Time>.

Message Type

LOG

Message Severity

['MAPS-2116 : CRITICAL', 'MAPS-2117 : ERROR', 'MAPS-2118 : WARNING', 'MAPS-2119 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

Recommended Action

Reseat the blade or reboot the switch.

MAPS-2120 to MAPS-2123**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>, Quiet Time=<Quiet Time>.

Message Type

LOG

Message Severity

['MAPS-2120 : CRITICAL', 'MAPS-2121 : ERROR', 'MAPS-2122 : WARNING', 'MAPS-2123 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

Recommended Action

Reseat the blade or reboot the switch.

MAPS-2124 to MAPS-2127**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>, Quiet Time=<Quiet Time>.

Message Type

LOG

Message Severity

['MAPS-2124 : CRITICAL', 'MAPS-2125 : ERROR', 'MAPS-2126 : WARNING', 'MAPS-2127 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

Recommended Action

Reseat the blade or reboot the switch.

MAPS-2128 to MAPS-2131**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>, Quiet Time=<Quiet Time>.

Message Type

LOG

Message Severity

['MAPS-2128 : CRITICAL', 'MAPS-2129 : ERROR', 'MAPS-2130 : WARNING', 'MAPS-2131 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

Recommended Action

Reseat the blade or reboot the switch.

MAPS-2132 to MAPS-2135**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

['MAPS-2132 : CRITICAL', 'MAPS-2133 : ERROR', 'MAPS-2134 : WARNING', 'MAPS-2135 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2136 to MAPS-2139

Message

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

['MAPS-2136 : CRITICAL', 'MAPS-2137 : ERROR', 'MAPS-2138 : WARNING', 'MAPS-2139 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2140 to MAPS-2143

Message

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>, Quiet Time=<Quiet Time>.

Message Type

LOG

Message Severity

['MAPS-2140 : CRITICAL', 'MAPS-2141 : ERROR', 'MAPS-2142 : WARNING', 'MAPS-2143 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

Recommended Action

The state of the circuit has changed for either of the reason that if the circuit has gone offline or it has come online. Check the connectivity between the circuit endpoints for reliability.

MAPS-2144 to MAPS-2147

Message

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>, Quiet Time=<Quiet Time>.

Message Type

LOG

Message Severity

['MAPS-2144 : CRITICAL', 'MAPS-2145 : ERROR', 'MAPS-2146 : WARNING', 'MAPS-2147 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

Recommended Action

High utilization may indicate the need for more bandwidth or parallel connections.

MAPS-2148 to MAPS-2151**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>, Quiet Time=<Quiet Time>.

Message Type

LOG

Message Severity

['MAPS-2148 : CRITICAL', 'MAPS-2149 : ERROR', 'MAPS-2150 : WARNING', 'MAPS-2151 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

Recommended Action

High packet loss may indicate a congested or unreliable intermediate link. If the issue persists then you need to work with the service provider.

MAPS-2152 to MAPS-2155**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>, Quiet Time=<Quiet Time>.

Message Type

LOG

Message Severity

['MAPS-2152 : CRITICAL', 'MAPS-2153 : ERROR', 'MAPS-2154 : WARNING', 'MAPS-2155 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

Recommended Action

Flash increases and decreases slightly with normal operation of the switch. Excessive permanent increases can lead to future problems. Remove some unwanted files to create some flash space. Execute the supportSave command to remove files from the kernel space.

MAPS-2156 to MAPS-2159**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>, Quiet Time=<Quiet Time>.

Message Type

LOG

Message Severity

['MAPS-2156 : CRITICAL', 'MAPS-2157 : ERROR', 'MAPS-2158 : WARNING', 'MAPS-2159 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

Recommended Action

This is an indication of excessive CPU intensive processes running on the switch. If the CPU usage level remains high without reducing, contact your switch support vendor.

MAPS-2160 to MAPS-2163**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>, Quiet Time=<Quiet Time>.

Message Type

LOG

Message Severity

['MAPS-2160 : CRITICAL', 'MAPS-2161 : ERROR', 'MAPS-2162 : WARNING', 'MAPS-2163 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

Recommended Action

This could be an indication of a possible memory leak if it is continuously increasing or if there are excessive processes running on a switch. If the memory usage does not decrease, contact your switch support vendor.

MAPS-2164 to MAPS-2167

Message

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>, Quiet Time=<Quiet Time>.

Message Type

LOG

Message Severity

['MAPS-2164 : CRITICAL', 'MAPS-2165 : ERROR', 'MAPS-2166 : WARNING', 'MAPS-2167 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

Recommended Action

Temperature changes can indicate a fan problem. Verify that the location temperature is within the operational range of the switch. Refer to the hardware reference manual for the environmental temperature range of your switch. If you receive a temperature-related message, check for an accompanying fan-related message and check fan performance. If all fans are functioning normally, check the climate control in your lab.

MAPS-2168 to MAPS-2171

Message

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>, Quiet Time=<Quiet Time>.

Message Type

LOG

Message Severity

['MAPS-2168 : CRITICAL', 'MAPS-2169 : ERROR', 'MAPS-2170 : WARNING', 'MAPS-2171 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

Recommended Action

If the power supply is functioning correctly, no action is required. If the power supply is not functioning correctly, verify that it is seated correctly in the chassis. Run the psShow command to view the status of the power supply. If the problem persists, replace the faulty power supply.

MAPS-2172 to MAPS-2175

Message

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>, Quiet Time=<Quiet Time>.

Message Type

LOG

Message Severity

['MAPS-2172 : CRITICAL', 'MAPS-2173 : ERROR', 'MAPS-2174 : WARNING', 'MAPS-2175 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

Recommended Action

Fan problems typically contribute to temperature problems. If the fan is functioning correctly, no action is required. If the fan is not functioning correctly, verify that it is seated correctly in the chassis. Run the fanShow command to view the status of the fan. If the problem persists, replace the faulty fan.

MAPS-2176 to MAPS-2179

Message

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

['MAPS-2176 : CRITICAL', 'MAPS-2177 : ERROR', 'MAPS-2178 : WARNING', 'MAPS-2179 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2180 to MAPS-2183

Message

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>, Quiet Time=<Quiet Time>.

Message Type

LOG

Message Severity

['MAPS-2180 : CRITICAL', 'MAPS-2181 : ERROR', 'MAPS-2182 : WARNING', 'MAPS-2183 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

Recommended Action

SFP state changes occur when the SFP is inserted or removed. If the SFP insertion or removal was not expected, take appropriate action based on the end-user policies for changes in the environment.

MAPS-2184 to MAPS-2187**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>, Quiet Time=<Quiet Time>.

Message Type

LOG

Message Severity

['MAPS-2184 : CRITICAL', 'MAPS-2185 : ERROR', 'MAPS-2186 : WARNING', 'MAPS-2187 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

Recommended Action

If the state is INSERTED, this means that the blade is inserted but not powered on. If the state is ON, this means that the blade has been powered on. If the state is OFF, this means that the blade has been powered off. For states INSERTED, ON and OFF, verify that the event was planned. If the state is FAULTY, this means that the blade has deteriorated into FAULTY state. Take appropriate action to repair or replace the faulty blade.

MAPS-2188 to MAPS-2191**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>, Quiet Time=<Quiet Time>.

Message Type

LOG

Message Severity

['MAPS-2188 : CRITICAL', 'MAPS-2189 : ERROR', 'MAPS-2190 : WARNING', 'MAPS-2191 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

Recommended Action

Verify that the event was planned. If the state is FAULTY, this means that the WWN card has deteriorated into FAULTY state. Take appropriate action to repair or replace the faulty WWN card.

MAPS-2192 to MAPS-2195**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>, Quiet Time=<Quiet Time>.

Message Type

LOG

Message Severity

['MAPS-2192 : CRITICAL', 'MAPS-2193 : ERROR', 'MAPS-2194 : WARNING', 'MAPS-2195 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

Recommended Action

Check the fan direction using chassis show command and fix the fan direction .

MAPS-2196 to MAPS-2199**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>, Quiet Time=<Quiet Time>.

Message Type

LOG

Message Severity

['MAPS-2196 : CRITICAL', 'MAPS-2197 : ERROR', 'MAPS-2198 : WARNING', 'MAPS-2199 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

Recommended Action

Telnet violations indicate that a Telnet connection request has been received from an unauthorized IP address. The IP ACL (via ipfilter) policy contains a list of internet protocol (IP) addresses that are authorized/denied to establish

Telnet connections to switches in the fabric. Refer to the master log to determine the IP address that sent the request. Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

MAPS-2200 to MAPS-2203

Message

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>, Quiet Time=<Quiet Time>.

Message Type

LOG

Message Severity

['MAPS-2200 : CRITICAL', 'MAPS-2201 : ERROR', 'MAPS-2202 : WARNING', 'MAPS-2203 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

Recommended Action

HTTP violations indicate that a HTTP connection request has been received from an unauthorized IP address. The IP ACL (via ipfilter) policy contains a list of internet protocol (IP) addresses that are authorized/denied to establish HTTP connections to switches in the fabric. Refer to the master log to determine the IP address that sent the request. Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

MAPS-2204 to MAPS-2207

Message

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>, Quiet Time=<Quiet Time>.

Message Type

LOG

Message Severity

['MAPS-2204 : CRITICAL', 'MAPS-2205 : ERROR', 'MAPS-2206 : WARNING', 'MAPS-2207 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

Recommended Action

SCC violations indicate that an unauthorized switch tried to join the fabric. The SCC_POLICY contains a list of switches by World Wide Name (WWN) that are allowed to be members of a fabric. Refer to the master log to determine the WWN

of the device that sent the request. Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

MAPS-2208 to MAPS-2211

Message

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>, Quiet Time=<Quiet Time>.

Message Type

LOG

Message Severity

['MAPS-2208 : CRITICAL', 'MAPS-2209 : ERROR', 'MAPS-2210 : WARNING', 'MAPS-2211 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

Recommended Action

DCC violations indicate that an unauthorized device tried to join the fabric. The DCC_POLICY allows for the specification of rules for binding device ports (typically HBA ports) to specific switch ports. DCC policies ensure that whenever a device performs a fabric login (FLOGI) request, the World Wide Name (WWN) specified in the FLOGI is validated to be connected to the authorized port. Enforcement for private loop devices not performing FLOGI is done through the name server. Refer to the master log to determine the device WWN, switch WWN, and switch port. Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

MAPS-2212 to MAPS-2215

Message

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>, Quiet Time=<Quiet Time>.

Message Type

LOG

Message Severity

['MAPS-2212 : CRITICAL', 'MAPS-2213 : ERROR', 'MAPS-2214 : WARNING', 'MAPS-2215 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

Recommended Action

Login violations indicate that a user login failure has been detected in one of the following applications – SSH, Telnet, ReST and WebEM. Refer to the master log to determine the IP location of the login attempt. Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

MAPS-2216 to MAPS-2219**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

['MAPS-2216 : CRITICAL', 'MAPS-2217 : ERROR', 'MAPS-2218 : WARNING', 'MAPS-2219 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

Recommended Action

This violation indicates that a packet with an invalid certificate has been received from the primary fabric configuration server (FCS). Before a new primary FCS switch sends any configuration data to any switch in the fabric, it first sends its certificate to all the switches in the fabric. The receiving switch has to verify that the sender is the primary FCS switch and its certificate is signed by the Root CA recognized by the receiving switch. This counter keeps track of the number of packets received with invalid certificates. Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

MAPS-2220 to MAPS-2223**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>, Quiet Time=<Quiet Time>.

Message Type

LOG

Message Severity

['MAPS-2220 : CRITICAL', 'MAPS-2221 : ERROR', 'MAPS-2222 : WARNING', 'MAPS-2223 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

Recommended Action

TS violations indicate that the Time sync up on this switch has been missed for two polling cycles (128 seconds) for 19 continuous intervals. Check the fabric show output on current switch and primary/principal switch, verify the differences. Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

MAPS-2224 to MAPS-2227**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>, Quiet Time=<Quiet Time>.

Message Type

LOG

Message Severity

['MAPS-2224 : CRITICAL', 'MAPS-2225 : ERROR', 'MAPS-2226 : WARNING', 'MAPS-2227 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

Recommended Action

This counter keeps track of the number of authentication failures during port bring up. Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

MAPS-2228 to MAPS-2231**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

['MAPS-2228 : CRITICAL', 'MAPS-2229 : ERROR', 'MAPS-2230 : WARNING', 'MAPS-2231 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

Recommended Action

This counter records how often the switch loses contact with the primary fabric configuration server (FCS) switch. When the primary FCS switch in the fabric sends its certificate to a switch, the receiving switch saves the World Wide Name

(WWN) of that primary FCS switch. If a secure switch finds that there are no FCSs in the fabric, but it still has the WWN of the last primary FCS switch, it increments this counter and resets the WWN of the primary FCS to all zeroes. Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

MAPS-2232 to MAPS-2235

Message

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

['MAPS-2232 : CRITICAL', 'MAPS-2233 : ERROR', 'MAPS-2234 : WARNING', 'MAPS-2235 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

Recommended Action

This violation indicates the number of secure switches with different version stamps have been detected. When a switch is in secure mode, it connects only to another switch that is in secure mode and has a compatible security database. A compatible security database means that the version stamp and fabric configuration server (FCS) policy matches exactly. Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

MAPS-2236 to MAPS-2239

Message

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>, Quiet Time=<Quiet Time>.

Message Type

LOG

Message Severity

['MAPS-2236 : CRITICAL', 'MAPS-2237 : ERROR', 'MAPS-2238 : WARNING', 'MAPS-2239 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

Recommended Action

This counter keeps track of the number of command violations on a non-primary switch in a FCS configuration. Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

MAPS-2240 to MAPS-2243**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>, Quiet Time=<Quiet Time>.

Message Type

LOG

Message Severity

['MAPS-2240 : CRITICAL', 'MAPS-2241 : ERROR', 'MAPS-2242 : WARNING', 'MAPS-2243 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

Recommended Action

This alert keeps track the number of days pending before the certificate expiry. Generate/Install new security certificate before the certificate expiry date. Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

MAPS-2244 to MAPS-2247**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>, Quiet Time=<Quiet Time>.

Message Type

LOG

Message Severity

['MAPS-2244 : CRITICAL', 'MAPS-2245 : ERROR', 'MAPS-2246 : WARNING', 'MAPS-2247 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

Recommended Action

This alert provides the number of expired certificates. Replace the expired certificates by generating/installing the new certificates to resolve the issue. Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

MAPS-2248 to MAPS-2251**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

['MAPS-2248 : CRITICAL', 'MAPS-2249 : ERROR', 'MAPS-2250 : WARNING', 'MAPS-2251 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2252 to MAPS-2255**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

['MAPS-2252 : CRITICAL', 'MAPS-2253 : ERROR', 'MAPS-2254 : WARNING', 'MAPS-2255 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2256 to MAPS-2259**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

['MAPS-2256 : CRITICAL', 'MAPS-2257 : ERROR', 'MAPS-2258 : WARNING', 'MAPS-2259 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2260 to MAPS-2263**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>, Quiet Time=<Quiet Time>.

Message Type

LOG

Message Severity

['MAPS-2260 : CRITICAL', 'MAPS-2261 : ERROR', 'MAPS-2262 : WARNING', 'MAPS-2263 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

Recommended Action

Frequent fluctuations in SFP temperature may indicate a deteriorating SFP. Verify that the switch is properly ventilated or replace the SFP.

MAPS-2264 to MAPS-2267**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>, Quiet Time=<Quiet Time>.

Message Type

LOG

Message Severity

['MAPS-2264 : CRITICAL', 'MAPS-2265 : ERROR', 'MAPS-2266 : WARNING', 'MAPS-2267 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

Recommended Action

If the supplied voltage of the SFP transceiver is outside of the normal range, this may indicate a hardware failure. Frequent voltage fluctuations indicate that the SFP is deteriorating. Verify that your optical components are clean and function properly. Replace deteriorating SFPs. Check for damage from heat or age.

MAPS-2268 to MAPS-2271**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>, Quiet Time=<Quiet Time>.

Message Type

LOG

Message Severity

['MAPS-2268 : CRITICAL', 'MAPS-2269 : ERROR', 'MAPS-2270 : WARNING', 'MAPS-2271 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

Recommended Action

If the supplied current of the SFP transceiver is outside of the normal range, this may indicate a hardware failure. If the message persists, replace the SFP.

MAPS-2272 to MAPS-2275**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>, Quiet Time=<Quiet Time>.

Message Type

LOG

Message Severity

['MAPS-2272 : CRITICAL', 'MAPS-2273 : ERROR', 'MAPS-2274 : WARNING', 'MAPS-2275 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

Recommended Action

The receive performance area measures the amount of incoming laser to help you determine if the SFP is in good working condition or not. If the counter often exceeds the threshold, the SFP is deteriorating. Incoming laser fluctuations usually

indicate a deteriorating SFP. If the message persists, verify that your optical components are clean and function properly. Replace deteriorating cables or SFPs. Check for damage from heat or age.

MAPS-2276 to MAPS-2279

Message

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>, Quiet Time=<Quiet Time>.

Message Type

LOG

Message Severity

['MAPS-2276 : CRITICAL', 'MAPS-2277 : ERROR', 'MAPS-2278 : WARNING', 'MAPS-2279 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

Recommended Action

The transmit performance area measures the amount of outgoing laser to help you determine if the SFP is in good working condition or not. If the counter often exceeds the threshold, the SFP is deteriorating. Transmitting laser fluctuations usually indicate a deteriorating SFP. If the message persists, verify that your optical components are clean and function properly. Replace deteriorating SFPs. Check for damage from heat or age.

MAPS-2280 to MAPS-2283

Message

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>, Quiet Time=<Quiet Time>.

Message Type

LOG

Message Severity

['MAPS-2280 : CRITICAL', 'MAPS-2281 : ERROR', 'MAPS-2282 : WARNING', 'MAPS-2283 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

Recommended Action

If continuous or repeated violations occur, replace the SFP before it deteriorates. A high value indicates that the SFP is nearing the maximum lifetime of use.

MAPS-2284 to MAPS-2287

Message

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>, Quiet Time=<Quiet Time>.

Message Type

LOG

Message Severity

['MAPS-2284 : CRITICAL', 'MAPS-2285 : ERROR', 'MAPS-2286 : WARNING', 'MAPS-2287 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

Recommended Action

Replace the FRU which contains the faulty temperature sensor.

MAPS-2288 to MAPS-2291

Message

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>, Quiet Time=<Quiet Time>.

Message Type

LOG

Message Severity

['MAPS-2288 : CRITICAL', 'MAPS-2289 : ERROR', 'MAPS-2290 : WARNING', 'MAPS-2291 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

Recommended Action

Replace the faulty power supply.

MAPS-2292 to MAPS-2295

Message

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>, Quiet Time=<Quiet Time>.

Message Type

LOG

Message Severity

['MAPS-2292 : CRITICAL', 'MAPS-2293 : ERROR', 'MAPS-2294 : WARNING', 'MAPS-2295 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

Recommended Action

Replace the faulty fan.

MAPS-2296 to MAPS-2299

Message

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>, Quiet Time=<Quiet Time>.

Message Type

LOG

Message Severity

['MAPS-2296 : CRITICAL', 'MAPS-2297 : ERROR', 'MAPS-2298 : WARNING', 'MAPS-2299 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

Recommended Action

Replace any faulty or deteriorating SFPs.

MAPS-2300 to MAPS-2303

Message

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>, Quiet Time=<Quiet Time>.

Message Type

LOG

Message Severity

['MAPS-2300 : CRITICAL', 'MAPS-2301 : ERROR', 'MAPS-2302 : WARNING', 'MAPS-2303 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

Recommended Action

Insert SFPs into ports where the FRU is missing or increase the threshold for missing SFPs.

MAPS-2304 to MAPS-2307**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>, Quiet Time=<Quiet Time>.

Message Type

LOG

Message Severity

['MAPS-2304 : CRITICAL', 'MAPS-2305 : ERROR', 'MAPS-2306 : WARNING', 'MAPS-2307 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

Recommended Action

The number of faulty port blades has exceeded the defined threshold. Replace the faulty port blade.

MAPS-2308 to MAPS-2311**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>, Quiet Time=<Quiet Time>.

Message Type

LOG

Message Severity

['MAPS-2308 : CRITICAL', 'MAPS-2309 : ERROR', 'MAPS-2310 : WARNING', 'MAPS-2311 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

Recommended Action

Replace any faulty or deteriorating SFPs or resolve link errors causing marginal port state.

MAPS-2312 to MAPS-2315

Message

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>, Quiet Time=<Quiet Time>.

Message Type

LOG

Message Severity

['MAPS-2312 : CRITICAL', 'MAPS-2313 : ERROR', 'MAPS-2314 : WARNING', 'MAPS-2315 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

Recommended Action

Resolve any port segmentation or disabled port issues. Take necessary action to bring the ports online.

MAPS-2316 to MAPS-2319

Message

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>, Quiet Time=<Quiet Time>.

Message Type

LOG

Message Severity

['MAPS-2316 : CRITICAL', 'MAPS-2317 : ERROR', 'MAPS-2318 : WARNING', 'MAPS-2319 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

Recommended Action

E_Ports go down each time you remove a cable or small form-factor pluggable (SFP). SFP failures also cause E_Ports to go down. E_Port downs might be caused by transient errors. Check both ends of the physical connection and verify that the SFPs and cables are functioning properly.

MAPS-2320 to MAPS-2323

Message

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>, Quiet Time=<Quiet Time>.

Message Type

LOG

Message Severity

['MAPS-2320 : CRITICAL', 'MAPS-2321 : ERROR', 'MAPS-2322 : WARNING', 'MAPS-2323 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

Recommended Action

The following occurrences can cause a fabric reconfiguration: Two switches with the same domain ID have connected to one another, two fabrics have joined, an E_Port has gone offline, or a principal link has segmented from the fabric. Verify that the cable is properly connected at both ends. Verify that the small form-factor pluggables (SFPs) have not become faulty. An inexplicable fabric reconfiguration might be a transient error and might not require troubleshooting.

MAPS-2324 to MAPS-2327**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>, Quiet Time=<Quiet Time>.

Message Type

LOG

Message Severity

['MAPS-2324 : CRITICAL', 'MAPS-2325 : ERROR', 'MAPS-2326 : WARNING', 'MAPS-2327 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

Recommended Action

Domain ID changes occur when there is a conflict of domain IDs in a single fabric and the principal switch has to assign another domain ID to the switch, or unintentional configuration of persistent domain IDs. If the change is not an expected event in the environment, confirm fabric state and device connectivity. Correcting the domain ID may be necessary in environments that utilize domain/area zoning architecture.

MAPS-2328 to MAPS-2331**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>, Quiet Time=<Quiet Time>.

Message Type

LOG

Message Severity

['MAPS-2328 : CRITICAL', 'MAPS-2329 : ERROR', 'MAPS-2330 : WARNING', 'MAPS-2331 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

Recommended Action

Segmentation changes might occur due to the following reasons: Zone conflicts, domain conflicts, segmentation of the principal link between two switches, or incompatible link parameters. During E_Port initialization, ports exchange link parameters. Rarely, incompatible parameters result in segmentation. Correct the segmentation that is identified. If it is indeterminable, contact your switch support vendor for assistance.

MAPS-2332 to MAPS-2335**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

['MAPS-2332 : CRITICAL', 'MAPS-2333 : ERROR', 'MAPS-2334 : WARNING', 'MAPS-2335 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2336 to MAPS-2339**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>, Quiet Time=<Quiet Time>.

Message Type

LOG

Message Severity

['MAPS-2336 : CRITICAL', 'MAPS-2337 : ERROR', 'MAPS-2338 : WARNING', 'MAPS-2339 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

Recommended Action

Zone changes occur when there is a change to the effective zone configuration. If the zone changes performed were not expected, respond as appropriate based on current end-user policies for zone changes.

MAPS-2340 to MAPS-2343**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>, Quiet Time=<Quiet Time>.

Message Type

LOG

Message Severity

['MAPS-2340 : CRITICAL', 'MAPS-2341 : ERROR', 'MAPS-2342 : WARNING', 'MAPS-2343 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

Recommended Action

Fabric logins occur when a port or device initializes with the fabric. The event is called fabric login (FLOGI). If the fabric login is not expected, confirm if there should be a device logged in on that port. Take appropriate action based on fabric defined policies.

MAPS-2344 to MAPS-2347**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>, Quiet Time=<Quiet Time>.

Message Type

LOG

Message Severity

['MAPS-2344 : CRITICAL', 'MAPS-2345 : ERROR', 'MAPS-2346 : WARNING', 'MAPS-2347 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

Recommended Action

Reduce the number of hosts or targets attached to the Layer 2 fabric to a value lower than the configured limit.

MAPS-2348 to MAPS-2351**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>, Quiet Time=<Quiet Time>.

Message Type

LOG

Message Severity

['MAPS-2348 : CRITICAL', 'MAPS-2349 : ERROR', 'MAPS-2350 : WARNING', 'MAPS-2351 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

Recommended Action

Reduce the number of imported hosts or targets within a meta-SAN to the recommended scalability limit.

MAPS-2352 to MAPS-2355**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>, Quiet Time=<Quiet Time>.

Message Type

LOG

Message Severity

['MAPS-2352 : CRITICAL', 'MAPS-2353 : ERROR', 'MAPS-2354 : WARNING', 'MAPS-2355 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

Recommended Action

Reduce the size of zoning configuration to the recommended scalability limit.

MAPS-2356 to MAPS-2359

Message

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>, Quiet Time=<Quiet Time>.

Message Type

LOG

Message Severity

['MAPS-2356 : CRITICAL', 'MAPS-2357 : ERROR', 'MAPS-2358 : WARNING', 'MAPS-2359 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

Recommended Action

Reduce the number of Fiber Channel Routers in the backbone fabric to the recommended scalability limit.

MAPS-2360 to MAPS-2363

Message

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>, Quiet Time=<Quiet Time>.

Message Type

LOG

Message Severity

['MAPS-2360 : CRITICAL', 'MAPS-2361 : ERROR', 'MAPS-2362 : WARNING', 'MAPS-2363 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

Recommended Action

Make sure that the blade is seated correctly. If the blade is seated correctly, execute the `diagPost`

MAPS-2364 to MAPS-2367

Message

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>, Quiet Time=<Quiet Time>.

Message Type

LOG

Message Severity

['MAPS-2364 : CRITICAL', 'MAPS-2365 : ERROR', 'MAPS-2366 : WARNING', 'MAPS-2367 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

Recommended Action

Verify both CP blades have compatible firmware levels. Replace any faulty CP blades.

MAPS-2368 to MAPS-2371**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>, Quiet Time=<Quiet Time>.

Message Type

LOG

Message Severity

['MAPS-2368 : CRITICAL', 'MAPS-2369 : ERROR', 'MAPS-2370 : WARNING', 'MAPS-2371 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

Recommended Action

The number of faulty WWN cards has exceeded the defined threshold. Replace the faulty WWN card.

MAPS-2372 to MAPS-2375**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

['MAPS-2372 : CRITICAL', 'MAPS-2373 : ERROR', 'MAPS-2374 : WARNING', 'MAPS-2375 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2376 to MAPS-2379**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

['MAPS-2376 : CRITICAL', 'MAPS-2377 : ERROR', 'MAPS-2378 : WARNING', 'MAPS-2379 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2380 to MAPS-2383**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

['MAPS-2380 : CRITICAL', 'MAPS-2381 : ERROR', 'MAPS-2382 : WARNING', 'MAPS-2383 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2384 to MAPS-2387**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

['MAPS-2384 : CRITICAL', 'MAPS-2385 : ERROR', 'MAPS-2386 : WARNING', 'MAPS-2387 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2388 to MAPS-2391**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

['MAPS-2388 : CRITICAL', 'MAPS-2389 : ERROR', 'MAPS-2390 : WARNING', 'MAPS-2391 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2392 to MAPS-2395**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

['MAPS-2392 : CRITICAL', 'MAPS-2393 : ERROR', 'MAPS-2394 : WARNING', 'MAPS-2395 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2396 to MAPS-2399**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

['MAPS-2396 : CRITICAL', 'MAPS-2397 : ERROR', 'MAPS-2398 : WARNING', 'MAPS-2399 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2400 to MAPS-2403**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

['MAPS-2400 : CRITICAL', 'MAPS-2401 : ERROR', 'MAPS-2402 : WARNING', 'MAPS-2403 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2404 to MAPS-2407**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

['MAPS-2404 : CRITICAL', 'MAPS-2405 : ERROR', 'MAPS-2406 : WARNING', 'MAPS-2407 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2408 to MAPS-2411

Message

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>, Quiet Time=<Quiet Time>.

Message Type

LOG

Message Severity

['MAPS-2408 : CRITICAL', 'MAPS-2409 : ERROR', 'MAPS-2410 : WARNING', 'MAPS-2411 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

Recommended Action

Check Ethernet management port physical connection and IP network configuration to ensure the stability.

MAPS-2412 to MAPS-2415

Message

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>, Quiet Time=<Quiet Time>.

Message Type

LOG

Message Severity

['MAPS-2412 : CRITICAL', 'MAPS-2413 : ERROR', 'MAPS-2414 : WARNING', 'MAPS-2415 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

Recommended Action

The state of the tunnel has changed by transitioning to online or offline. Check the connectivity between the tunnel endpoints for reliability.

MAPS-2416 to MAPS-2419

Message

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>, Quiet Time=<Quiet Time>.

Message Type

LOG

Message Severity

['MAPS-2416 : CRITICAL', 'MAPS-2417 : ERROR', 'MAPS-2418 : WARNING', 'MAPS-2419 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

Recommended Action

High utilization may indicate the need for more bandwidth or parallel connections.

MAPS-2420 to MAPS-2423**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>, Quiet Time=<Quiet Time>.

Message Type

LOG

Message Severity

['MAPS-2420 : CRITICAL', 'MAPS-2421 : ERROR', 'MAPS-2422 : WARNING', 'MAPS-2423 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

Recommended Action

High utilization may indicate the need for more bandwidth or parallel connections.

MAPS-2424 to MAPS-2427**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>, Quiet Time=<Quiet Time>.

Message Type

LOG

Message Severity

['MAPS-2424 : CRITICAL', 'MAPS-2425 : ERROR', 'MAPS-2426 : WARNING', 'MAPS-2427 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

Recommended Action

High packet loss may indicate a congested or unreliable intermediate link. If the issue persists then you need to work with the service provider.

MAPS-2428 to MAPS-2431**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>, Quiet Time=<Quiet Time>.

Message Type

LOG

Message Severity

['MAPS-2428 : CRITICAL', 'MAPS-2429 : ERROR', 'MAPS-2430 : WARNING', 'MAPS-2431 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

Recommended Action

The RTT of the tunnel / circuit has exceeded the allowable threshold. Check the network path for possible network disruptions or route changes.

MAPS-2432 to MAPS-2435**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>, Quiet Time=<Quiet Time>.

Message Type

LOG

Message Severity

['MAPS-2432 : CRITICAL', 'MAPS-2433 : ERROR', 'MAPS-2434 : WARNING', 'MAPS-2435 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

Recommended Action

The RTT variance has exceeded the allowable threshold. Check the network path for possible network disruptions or congestion.

MAPS-2436 to MAPS-2439**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

['MAPS-2436 : CRITICAL', 'MAPS-2437 : ERROR', 'MAPS-2438 : WARNING', 'MAPS-2439 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2440 to MAPS-2443**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>, Quiet Time=<Quiet Time>.

Message Type

LOG

Message Severity

['MAPS-2440 : CRITICAL', 'MAPS-2441 : ERROR', 'MAPS-2442 : WARNING', 'MAPS-2443 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

Recommended Action

High utilization may indicate the need for more bandwidth or parallel connections.

MAPS-2444 to MAPS-2447**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>, Quiet Time=<Quiet Time>.

Message Type

LOG

Message Severity

['MAPS-2444 : CRITICAL', 'MAPS-2445 : ERROR', 'MAPS-2446 : WARNING', 'MAPS-2447 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

Recommended Action

High packet loss may indicate a congested or unreliable intermediate link. If the issue persists then you need to work with the service provider.

MAPS-2448 to MAPS-2451**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

['MAPS-2448 : CRITICAL', 'MAPS-2449 : ERROR', 'MAPS-2450 : WARNING', 'MAPS-2451 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2452 to MAPS-2455**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

['MAPS-2452 : CRITICAL', 'MAPS-2453 : ERROR', 'MAPS-2454 : WARNING', 'MAPS-2455 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2456 to MAPS-2459

Message

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

['MAPS-2456 : CRITICAL', 'MAPS-2457 : ERROR', 'MAPS-2458 : WARNING', 'MAPS-2459 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2460 to MAPS-2463

Message

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

['MAPS-2460 : CRITICAL', 'MAPS-2461 : ERROR', 'MAPS-2462 : WARNING', 'MAPS-2463 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2464 to MAPS-2467

Message

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

['MAPS-2464 : CRITICAL', 'MAPS-2465 : ERROR', 'MAPS-2466 : WARNING', 'MAPS-2467 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2468 to MAPS-2471**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

['MAPS-2468 : CRITICAL', 'MAPS-2469 : ERROR', 'MAPS-2470 : WARNING', 'MAPS-2471 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2472 to MAPS-2475**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

['MAPS-2472 : CRITICAL', 'MAPS-2473 : ERROR', 'MAPS-2474 : WARNING', 'MAPS-2475 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2476 to MAPS-2479**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

['MAPS-2476 : CRITICAL', 'MAPS-2477 : ERROR', 'MAPS-2478 : WARNING', 'MAPS-2479 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2480 to MAPS-2483**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

['MAPS-2480 : CRITICAL', 'MAPS-2481 : ERROR', 'MAPS-2482 : WARNING', 'MAPS-2483 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2484 to MAPS-2487**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

['MAPS-2484 : CRITICAL', 'MAPS-2485 : ERROR', 'MAPS-2486 : WARNING', 'MAPS-2487 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2488 to MAPS-2491**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

['MAPS-2488 : CRITICAL', 'MAPS-2489 : ERROR', 'MAPS-2490 : WARNING', 'MAPS-2491 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2492 to MAPS-2495**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

['MAPS-2492 : CRITICAL', 'MAPS-2493 : ERROR', 'MAPS-2494 : WARNING', 'MAPS-2495 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2496 to MAPS-2499**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

['MAPS-2496 : CRITICAL', 'MAPS-2497 : ERROR', 'MAPS-2498 : WARNING', 'MAPS-2499 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2500 to MAPS-2503

Message

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

['MAPS-2500 : CRITICAL', 'MAPS-2501 : ERROR', 'MAPS-2502 : WARNING', 'MAPS-2503 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2504 to MAPS-2507

Message

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

['MAPS-2504 : CRITICAL', 'MAPS-2505 : ERROR', 'MAPS-2506 : WARNING', 'MAPS-2507 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2508 to MAPS-2511

Message

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

['MAPS-2508 : CRITICAL', 'MAPS-2509 : ERROR', 'MAPS-2510 : WARNING', 'MAPS-2511 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2512 to MAPS-2515**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

['MAPS-2512 : CRITICAL', 'MAPS-2513 : ERROR', 'MAPS-2514 : WARNING', 'MAPS-2515 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2516 to MAPS-2519**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

['MAPS-2516 : CRITICAL', 'MAPS-2517 : ERROR', 'MAPS-2518 : WARNING', 'MAPS-2519 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2520 to MAPS-2523**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

['MAPS-2520 : CRITICAL', 'MAPS-2521 : ERROR', 'MAPS-2522 : WARNING', 'MAPS-2523 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2524 to MAPS-2527**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

['MAPS-2524 : CRITICAL', 'MAPS-2525 : ERROR', 'MAPS-2526 : WARNING', 'MAPS-2527 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2528 to MAPS-2531**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

['MAPS-2528 : CRITICAL', 'MAPS-2529 : ERROR', 'MAPS-2530 : WARNING', 'MAPS-2531 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2532 to MAPS-2535**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

['MAPS-2532 : CRITICAL', 'MAPS-2533 : ERROR', 'MAPS-2534 : WARNING', 'MAPS-2535 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2536 to MAPS-2539**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

['MAPS-2536 : CRITICAL', 'MAPS-2537 : ERROR', 'MAPS-2538 : WARNING', 'MAPS-2539 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2540 to MAPS-2543**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

['MAPS-2540 : CRITICAL', 'MAPS-2541 : ERROR', 'MAPS-2542 : WARNING', 'MAPS-2543 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2544 to MAPS-2547

Message

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

['MAPS-2544 : CRITICAL', 'MAPS-2545 : ERROR', 'MAPS-2546 : WARNING', 'MAPS-2547 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2548 to MAPS-2551

Message

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

['MAPS-2548 : CRITICAL', 'MAPS-2549 : ERROR', 'MAPS-2550 : WARNING', 'MAPS-2551 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2552 to MAPS-2555

Message

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

['MAPS-2552 : CRITICAL', 'MAPS-2553 : ERROR', 'MAPS-2554 : WARNING', 'MAPS-2555 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2556 to MAPS-2559**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

['MAPS-2556 : CRITICAL', 'MAPS-2557 : ERROR', 'MAPS-2558 : WARNING', 'MAPS-2559 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2560 to MAPS-2563**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

['MAPS-2560 : CRITICAL', 'MAPS-2561 : ERROR', 'MAPS-2562 : WARNING', 'MAPS-2563 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2564 to MAPS-2567**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

['MAPS-2564 : CRITICAL', 'MAPS-2565 : ERROR', 'MAPS-2566 : WARNING', 'MAPS-2567 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2568 to MAPS-2571**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

['MAPS-2568 : CRITICAL', 'MAPS-2569 : ERROR', 'MAPS-2570 : WARNING', 'MAPS-2571 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2572 to MAPS-2575**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

['MAPS-2572 : CRITICAL', 'MAPS-2573 : ERROR', 'MAPS-2574 : WARNING', 'MAPS-2575 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2576 to MAPS-2579**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

['MAPS-2576 : CRITICAL', 'MAPS-2577 : ERROR', 'MAPS-2578 : WARNING', 'MAPS-2579 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2580 to MAPS-2583**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

['MAPS-2580 : CRITICAL', 'MAPS-2581 : ERROR', 'MAPS-2582 : WARNING', 'MAPS-2583 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2584 to MAPS-2587**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

['MAPS-2584 : CRITICAL', 'MAPS-2585 : ERROR', 'MAPS-2586 : WARNING', 'MAPS-2587 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2588 to MAPS-2591

Message

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

['MAPS-2588 : CRITICAL', 'MAPS-2589 : ERROR', 'MAPS-2590 : WARNING', 'MAPS-2591 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2592 to MAPS-2595

Message

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

['MAPS-2592 : CRITICAL', 'MAPS-2593 : ERROR', 'MAPS-2594 : WARNING', 'MAPS-2595 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2596 to MAPS-2599

Message

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

['MAPS-2596 : CRITICAL', 'MAPS-2597 : ERROR', 'MAPS-2598 : WARNING', 'MAPS-2599 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2600 to MAPS-2603**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

['MAPS-2600 : CRITICAL', 'MAPS-2601 : ERROR', 'MAPS-2602 : WARNING', 'MAPS-2603 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2604 to MAPS-2607**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

['MAPS-2604 : CRITICAL', 'MAPS-2605 : ERROR', 'MAPS-2606 : WARNING', 'MAPS-2607 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2608 to MAPS-2611**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

['MAPS-2608 : CRITICAL', 'MAPS-2609 : ERROR', 'MAPS-2610 : WARNING', 'MAPS-2611 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2612 to MAPS-2615**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

['MAPS-2612 : CRITICAL', 'MAPS-2613 : ERROR', 'MAPS-2614 : WARNING', 'MAPS-2615 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2616 to MAPS-2619**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

['MAPS-2616 : CRITICAL', 'MAPS-2617 : ERROR', 'MAPS-2618 : WARNING', 'MAPS-2619 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2620 to MAPS-2623**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

['MAPS-2620 : CRITICAL', 'MAPS-2621 : ERROR', 'MAPS-2622 : WARNING', 'MAPS-2623 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2624 to MAPS-2627**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

['MAPS-2624 : CRITICAL', 'MAPS-2625 : ERROR', 'MAPS-2626 : WARNING', 'MAPS-2627 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2628 to MAPS-2631**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

['MAPS-2628 : CRITICAL', 'MAPS-2629 : ERROR', 'MAPS-2630 : WARNING', 'MAPS-2631 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2640 to MAPS-2643

Message

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

['MAPS-2640 : CRITICAL', 'MAPS-2641 : ERROR', 'MAPS-2642 : WARNING', 'MAPS-2643 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2648 to MAPS-2651

Message

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

['MAPS-2648 : CRITICAL', 'MAPS-2649 : ERROR', 'MAPS-2650 : WARNING', 'MAPS-2651 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2652 to MAPS-2655

Message

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

['MAPS-2652 : CRITICAL', 'MAPS-2653 : ERROR', 'MAPS-2654 : WARNING', 'MAPS-2655 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2656 to MAPS-2659**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

['MAPS-2656 : CRITICAL', 'MAPS-2657 : ERROR', 'MAPS-2658 : WARNING', 'MAPS-2659 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2660 to MAPS-2663**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

['MAPS-2660 : CRITICAL', 'MAPS-2661 : ERROR', 'MAPS-2662 : WARNING', 'MAPS-2663 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2664 to MAPS-2667**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

['MAPS-2664 : CRITICAL', 'MAPS-2665 : ERROR', 'MAPS-2666 : WARNING', 'MAPS-2667 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2668 to MAPS-2671**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>, Quiet Time=<Quiet Time>.

Message Type

LOG

Message Severity

['MAPS-2668 : CRITICAL', 'MAPS-2669 : ERROR', 'MAPS-2670 : WARNING', 'MAPS-2671 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

Recommended Action

Reduce the mirrored traffic or re-distribute the device connections to different slot/chip. The mirrored traffic can be reduced by creating the logicalgroup with selected F-Ports.

MAPS-2672 to MAPS-2675**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>, Quiet Time=<Quiet Time>.

Message Type

LOG

Message Severity

['MAPS-2672 : CRITICAL', 'MAPS-2673 : ERROR', 'MAPS-2674 : WARNING', 'MAPS-2675 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

Recommended Action

Increase Analytics Switch Link(ASL) trunk ports or add a new AMP to the fabric.

MAPS-2676 to MAPS-2679

Message

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

['MAPS-2676 : CRITICAL', 'MAPS-2677 : ERROR', 'MAPS-2678 : WARNING', 'MAPS-2679 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2680 to MAPS-2683

Message

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

['MAPS-2680 : CRITICAL', 'MAPS-2681 : ERROR', 'MAPS-2682 : WARNING', 'MAPS-2683 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2684 to MAPS-2687

Message

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

['MAPS-2684 : CRITICAL', 'MAPS-2685 : ERROR', 'MAPS-2686 : WARNING', 'MAPS-2687 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2688 to MAPS-2691**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

['MAPS-2688 : CRITICAL', 'MAPS-2689 : ERROR', 'MAPS-2690 : WARNING', 'MAPS-2691 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2692 to MAPS-2695**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

['MAPS-2692 : CRITICAL', 'MAPS-2693 : ERROR', 'MAPS-2694 : WARNING', 'MAPS-2695 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2696 to MAPS-2699**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

['MAPS-2696 : CRITICAL', 'MAPS-2697 : ERROR', 'MAPS-2698 : WARNING', 'MAPS-2699 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2700 to MAPS-2703**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>, Quiet Time=<Quiet Time>.

Message Type

LOG

Message Severity

['MAPS-2700 : CRITICAL', 'MAPS-2701 : ERROR', 'MAPS-2702 : WARNING', 'MAPS-2703 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

Recommended Action

High utilization may indicate the need for more bandwidth or parallel connections.

MAPS-2704 to MAPS-2707**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>, Quiet Time=<Quiet Time>.

Message Type

LOG

Message Severity

['MAPS-2704 : CRITICAL', 'MAPS-2705 : ERROR', 'MAPS-2706 : WARNING', 'MAPS-2707 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

Recommended Action

High utilization may indicate the need for more bandwidth or parallel connections.

MAPS-2708 to MAPS-2711

Message

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>, Quiet Time=<Quiet Time>.

Message Type

LOG

Message Severity

['MAPS-2708 : CRITICAL', 'MAPS-2709 : ERROR', 'MAPS-2710 : WARNING', 'MAPS-2711 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

Recommended Action

High packet loss may indicate a congested or unreliable intermediate link. If the issue persists then you need to work with the service provider.

MAPS-2712 to MAPS-2715

Message

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>, Quiet Time=<Quiet Time>.

Message Type

LOG

Message Severity

['MAPS-2712 : CRITICAL', 'MAPS-2713 : ERROR', 'MAPS-2714 : WARNING', 'MAPS-2715 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

Recommended Action

If problem persists, consult their network provider to look for network issues. Alternatively can use wtool (7840) to test network to look for network issues.

MAPS-2716 to MAPS-2719

Message

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>, Quiet Time=<Quiet Time>.

Message Type

LOG

Message Severity

['MAPS-2716 : CRITICAL', 'MAPS-2717 : ERROR', 'MAPS-2718 : WARNING', 'MAPS-2719 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

Recommended Action

If problem persists, consult their network provider to look for network issues. Alternatively can use wtool (7840) to test network to look for network issues.

MAPS-2720 to MAPS-2723**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

['MAPS-2720 : CRITICAL', 'MAPS-2721 : ERROR', 'MAPS-2722 : WARNING', 'MAPS-2723 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2724 to MAPS-2727**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

['MAPS-2724 : CRITICAL', 'MAPS-2725 : ERROR', 'MAPS-2726 : WARNING', 'MAPS-2727 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2728 to MAPS-2731

Message

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

['MAPS-2728 : CRITICAL', 'MAPS-2729 : ERROR', 'MAPS-2730 : WARNING', 'MAPS-2731 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2732 to MAPS-2735

Message

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

['MAPS-2732 : CRITICAL', 'MAPS-2733 : ERROR', 'MAPS-2734 : WARNING', 'MAPS-2735 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2736 to MAPS-2739

Message

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

['MAPS-2736 : CRITICAL', 'MAPS-2737 : ERROR', 'MAPS-2738 : WARNING', 'MAPS-2739 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2740 to MAPS-2743**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

['MAPS-2740 : CRITICAL', 'MAPS-2741 : ERROR', 'MAPS-2742 : WARNING', 'MAPS-2743 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2744 to MAPS-2747**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

['MAPS-2744 : CRITICAL', 'MAPS-2745 : ERROR', 'MAPS-2746 : WARNING', 'MAPS-2747 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2748 to MAPS-2751**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

['MAPS-2748 : CRITICAL', 'MAPS-2749 : ERROR', 'MAPS-2750 : WARNING', 'MAPS-2751 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2752 to MAPS-2755**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

['MAPS-2752 : CRITICAL', 'MAPS-2753 : ERROR', 'MAPS-2754 : WARNING', 'MAPS-2755 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2756 to MAPS-2759**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

['MAPS-2756 : CRITICAL', 'MAPS-2757 : ERROR', 'MAPS-2758 : WARNING', 'MAPS-2759 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2760 to MAPS-2763**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

['MAPS-2760 : CRITICAL', 'MAPS-2761 : ERROR', 'MAPS-2762 : WARNING', 'MAPS-2763 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2764 to MAPS-2767**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

['MAPS-2764 : CRITICAL', 'MAPS-2765 : ERROR', 'MAPS-2766 : WARNING', 'MAPS-2767 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2768 to MAPS-2771**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

['MAPS-2768 : CRITICAL', 'MAPS-2769 : ERROR', 'MAPS-2770 : WARNING', 'MAPS-2771 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2772 to MAPS-2775

Message

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

['MAPS-2772 : CRITICAL', 'MAPS-2773 : ERROR', 'MAPS-2774 : WARNING', 'MAPS-2775 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2776 to MAPS-2779

Message

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

['MAPS-2776 : CRITICAL', 'MAPS-2777 : ERROR', 'MAPS-2778 : WARNING', 'MAPS-2779 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2780 to MAPS-2783

Message

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

['MAPS-2780 : CRITICAL', 'MAPS-2781 : ERROR', 'MAPS-2782 : WARNING', 'MAPS-2783 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2784 to MAPS-2787**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

['MAPS-2784 : CRITICAL', 'MAPS-2785 : ERROR', 'MAPS-2786 : WARNING', 'MAPS-2787 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2788 to MAPS-2791**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

['MAPS-2788 : CRITICAL', 'MAPS-2789 : ERROR', 'MAPS-2790 : WARNING', 'MAPS-2791 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2792 to MAPS-2795**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

['MAPS-2792 : CRITICAL', 'MAPS-2793 : ERROR', 'MAPS-2794 : WARNING', 'MAPS-2795 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2796 to MAPS-2799**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

['MAPS-2796 : CRITICAL', 'MAPS-2797 : ERROR', 'MAPS-2798 : WARNING', 'MAPS-2799 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2800 to MAPS-2803**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

['MAPS-2800 : CRITICAL', 'MAPS-2801 : ERROR', 'MAPS-2802 : WARNING', 'MAPS-2803 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2804 to MAPS-2807**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

['MAPS-2804 : CRITICAL', 'MAPS-2805 : ERROR', 'MAPS-2806 : WARNING', 'MAPS-2807 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2808 to MAPS-2811**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

['MAPS-2808 : CRITICAL', 'MAPS-2809 : ERROR', 'MAPS-2810 : WARNING', 'MAPS-2811 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2812 to MAPS-2815**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

['MAPS-2812 : CRITICAL', 'MAPS-2813 : ERROR', 'MAPS-2814 : WARNING', 'MAPS-2815 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2816 to MAPS-2819

Message

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

['MAPS-2816 : CRITICAL', 'MAPS-2817 : ERROR', 'MAPS-2818 : WARNING', 'MAPS-2819 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2820 to MAPS-2823

Message

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

['MAPS-2820 : CRITICAL', 'MAPS-2821 : ERROR', 'MAPS-2822 : WARNING', 'MAPS-2823 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2824 to MAPS-2827

Message

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

['MAPS-2824 : CRITICAL', 'MAPS-2825 : ERROR', 'MAPS-2826 : WARNING', 'MAPS-2827 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2828 to MAPS-2831**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

['MAPS-2828 : CRITICAL', 'MAPS-2829 : ERROR', 'MAPS-2830 : WARNING', 'MAPS-2831 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2832 to MAPS-2835**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

['MAPS-2832 : CRITICAL', 'MAPS-2833 : ERROR', 'MAPS-2834 : WARNING', 'MAPS-2835 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2836 to MAPS-2839**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

['MAPS-2836 : CRITICAL', 'MAPS-2837 : ERROR', 'MAPS-2838 : WARNING', 'MAPS-2839 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2840 to MAPS-2843**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

['MAPS-2840 : CRITICAL', 'MAPS-2841 : ERROR', 'MAPS-2842 : WARNING', 'MAPS-2843 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2844 to MAPS-2847**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

['MAPS-2844 : CRITICAL', 'MAPS-2845 : ERROR', 'MAPS-2846 : WARNING', 'MAPS-2847 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2848 to MAPS-2851**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

['MAPS-2848 : CRITICAL', 'MAPS-2849 : ERROR', 'MAPS-2850 : WARNING', 'MAPS-2851 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2852 to MAPS-2855**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

['MAPS-2852 : CRITICAL', 'MAPS-2853 : ERROR', 'MAPS-2854 : WARNING', 'MAPS-2855 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2856 to MAPS-2859**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

['MAPS-2856 : CRITICAL', 'MAPS-2857 : ERROR', 'MAPS-2858 : WARNING', 'MAPS-2859 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2860 to MAPS-2863

Message

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

['MAPS-2860 : CRITICAL', 'MAPS-2861 : ERROR', 'MAPS-2862 : WARNING', 'MAPS-2863 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2864 to MAPS-2867

Message

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

['MAPS-2864 : CRITICAL', 'MAPS-2865 : ERROR', 'MAPS-2866 : WARNING', 'MAPS-2867 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2868 to MAPS-2871

Message

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

['MAPS-2868 : CRITICAL', 'MAPS-2869 : ERROR', 'MAPS-2870 : WARNING', 'MAPS-2871 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2872 to MAPS-2875**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

['MAPS-2872 : CRITICAL', 'MAPS-2873 : ERROR', 'MAPS-2874 : WARNING', 'MAPS-2875 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2876 to MAPS-2879**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

['MAPS-2876 : CRITICAL', 'MAPS-2877 : ERROR', 'MAPS-2878 : WARNING', 'MAPS-2879 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2880 to MAPS-2883**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

['MAPS-2880 : CRITICAL', 'MAPS-2881 : ERROR', 'MAPS-2882 : WARNING', 'MAPS-2883 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2884 to MAPS-2887**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

['MAPS-2884 : CRITICAL', 'MAPS-2885 : ERROR', 'MAPS-2886 : WARNING', 'MAPS-2887 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2888 to MAPS-2891**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

['MAPS-2888 : CRITICAL', 'MAPS-2889 : ERROR', 'MAPS-2890 : WARNING', 'MAPS-2891 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2892 to MAPS-2895**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

['MAPS-2892 : CRITICAL', 'MAPS-2893 : ERROR', 'MAPS-2894 : WARNING', 'MAPS-2895 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2896 to MAPS-2899**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

['MAPS-2896 : CRITICAL', 'MAPS-2897 : ERROR', 'MAPS-2898 : WARNING', 'MAPS-2899 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2900 to MAPS-2903**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

['MAPS-2900 : CRITICAL', 'MAPS-2901 : ERROR', 'MAPS-2902 : WARNING', 'MAPS-2903 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2904 to MAPS-2907

Message

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

['MAPS-2904 : CRITICAL', 'MAPS-2905 : ERROR', 'MAPS-2906 : WARNING', 'MAPS-2907 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2908 to MAPS-2911

Message

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

['MAPS-2908 : CRITICAL', 'MAPS-2909 : ERROR', 'MAPS-2910 : WARNING', 'MAPS-2911 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2912 to MAPS-2915

Message

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

['MAPS-2912 : CRITICAL', 'MAPS-2913 : ERROR', 'MAPS-2914 : WARNING', 'MAPS-2915 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2916 to MAPS-2919**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

['MAPS-2916 : CRITICAL', 'MAPS-2917 : ERROR', 'MAPS-2918 : WARNING', 'MAPS-2919 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2920 to MAPS-2923**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

['MAPS-2920 : CRITICAL', 'MAPS-2921 : ERROR', 'MAPS-2922 : WARNING', 'MAPS-2923 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2924 to MAPS-2927**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

['MAPS-2924 : CRITICAL', 'MAPS-2925 : ERROR', 'MAPS-2926 : WARNING', 'MAPS-2927 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2928 to MAPS-2931**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

['MAPS-2928 : CRITICAL', 'MAPS-2929 : ERROR', 'MAPS-2930 : WARNING', 'MAPS-2931 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2932 to MAPS-2935**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

['MAPS-2932 : CRITICAL', 'MAPS-2933 : ERROR', 'MAPS-2934 : WARNING', 'MAPS-2935 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2936 to MAPS-2939**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>, Quiet Time=<Quiet Time>.

Message Type

LOG

Message Severity

['MAPS-2936 : CRITICAL', 'MAPS-2937 : ERROR', 'MAPS-2938 : WARNING', 'MAPS-2939 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

Recommended Action

Modify the zone database to lower the zoned-in devices to reported device.

MAPS-2940 to MAPS-2943**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>, Quiet Time=<Quiet Time>.

Message Type

LOG

Message Severity

['MAPS-2940 : CRITICAL', 'MAPS-2941 : ERROR', 'MAPS-2942 : WARNING', 'MAPS-2943 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2944 to MAPS-2947**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>, Quiet Time=<Quiet Time>.

Message Type

LOG

Message Severity

['MAPS-2944 : CRITICAL', 'MAPS-2945 : ERROR', 'MAPS-2946 : WARNING', 'MAPS-2947 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2948 to MAPS-2951

Message

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>, Quiet Time=<Quiet Time>.

Message Type

LOG

Message Severity

['MAPS-2948 : CRITICAL', 'MAPS-2949 : ERROR', 'MAPS-2950 : WARNING', 'MAPS-2951 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2952 to MAPS-2955

Message

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>, Quiet Time=<Quiet Time>.

Message Type

LOG

Message Severity

['MAPS-2952 : CRITICAL', 'MAPS-2953 : ERROR', 'MAPS-2954 : WARNING', 'MAPS-2955 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2956 to MAPS-2959

Message

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>, Quiet Time=<Quiet Time>.

Message Type

LOG

Message Severity

['MAPS-2956 : CRITICAL', 'MAPS-2957 : ERROR', 'MAPS-2958 : WARNING', 'MAPS-2959 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

Recommended Action

Either no action is required or if you need more flows then add new blade or system.

MAPS-2960 to MAPS-2963**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

['MAPS-2960 : CRITICAL', 'MAPS-2961 : ERROR', 'MAPS-2962 : WARNING', 'MAPS-2963 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2964 to MAPS-2967**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type

LOG

Message Severity

['MAPS-2964 : CRITICAL', 'MAPS-2965 : ERROR', 'MAPS-2966 : WARNING', 'MAPS-2967 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-2968 to MAPS-2971**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>, Quiet Time=<Quiet Time>.

Message Type

LOG

Message Severity

['MAPS-2968 : CRITICAL', 'MAPS-2969 : ERROR', 'MAPS-2970 : WARNING', 'MAPS-2971 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

Recommended Action

IO exchange completion is taking more than configured threshold. This could happen due to various reasons like host/target mis-configuration, performance issues on the host/target devices, congestion in the fabric due to slow drain devices etc. Please check for other MAPS alerts related to port errors or credit stall issues.

MAPS-2972 to MAPS-2975**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>, Quiet Time=<Quiet Time>.

Message Type

LOG

Message Severity

['MAPS-2972 : CRITICAL', 'MAPS-2973 : ERROR', 'MAPS-2974 : WARNING', 'MAPS-2975 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

Recommended Action

IO exchange completion is taking more than configured threshold. This could happen due to various reasons like host/target mis-configuration, performance issues on the host/target devices, congestion in the fabric due to slow drain devices etc. Please check for other MAPS alerts related to port errors or credit stall issues.

MAPS-2976 to MAPS-2979**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>, Quiet Time=<Quiet Time>.

Message Type

LOG

Message Severity

['MAPS-2976 : CRITICAL', 'MAPS-2977 : ERROR', 'MAPS-2978 : WARNING', 'MAPS-2979 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

Recommended Action

IO exchange first response from Target is taking more than configured threshold. This could happen due to various reasons like host/target mis-configuration, performance issues on the host/target devices, congestion in the fabric due to slow drain devices etc. Please check for other MAPS alerts related to port errors or credit stall issues.

MAPS-2980 to MAPS-2983**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>, Quiet Time=<Quiet Time>.

Message Type

LOG

Message Severity

['MAPS-2980 : CRITICAL', 'MAPS-2981 : ERROR', 'MAPS-2982 : WARNING', 'MAPS-2983 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

Recommended Action

IO exchange first response from Target is taking more than configured threshold. This could happen due to various reasons like host/target mis-configuration, performance issues on the host/target devices, congestion in the fabric due to slow drain devices etc. Please check for other MAPS alerts related to port errors or credit stall issues.

MAPS-2992 to MAPS-2995**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>, Quiet Time=<Quiet Time>.

Message Type

LOG

Message Severity

['MAPS-2992 : CRITICAL', 'MAPS-2993 : ERROR', 'MAPS-2994 : WARNING', 'MAPS-2995 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

Recommended Action

Outstanding IOs on Target exceeded threshold. This could happen due to various reasons like host/target mis-configuration, performance issues on the host/target devices, congestion in the fabric due to slow drain devices etc. Please check for other MAPS alerts related to port errors or credit stall issues.

MAPS-2996 to MAPS-2999**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>, Quiet Time=<Quiet Time>.

Message Type

LOG

Message Severity

['MAPS-2996 : CRITICAL', 'MAPS-2997 : ERROR', 'MAPS-2998 : WARNING', 'MAPS-2999 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

Recommended Action

Outstanding IOs on Target exceeded threshold. This could happen due to various reasons like host/target mis-configuration, performance issues on the host/target devices, congestion in the fabric due to slow drain devices etc. Please check for other MAPS alerts related to port errors or credit stall issues.

MAPS-3000 to MAPS-3003**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>, Quiet Time=<Quiet Time>.

Message Type

LOG

Message Severity

['MAPS-3000 : CRITICAL', 'MAPS-3001 : ERROR', 'MAPS-3002 : WARNING', 'MAPS-3003 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-3004 to MAPS-3007

Message

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>, Quiet Time=<Quiet Time>.

Message Type

LOG

Message Severity

['MAPS-3004 : CRITICAL', 'MAPS-3005 : ERROR', 'MAPS-3006 : WARNING', 'MAPS-3007 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

Recommended Action

Customer can address the issue as follows: a) for IMBALANCED alert: i. Customers should turn on the RE_BALANCE automatic action if it is not already turned on. ii. Customers should do the rebalance operation manually using devicelogin command, if the IMBALANCED state persists. iii. If all the ports are heavily utilized then plan to add another link between switch and Cisco FI. b) BALANCED_FAILED alert: i. Customers should do the rebalance operation manually using devicelogin command. ii. If all the ports are heavily utilized then plan to add another link between switch and Cisco FI. c) BALANCED alert: i. No action is needed.

MAPS-3008 to MAPS-3011

Message

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>, Quiet Time=<Quiet Time>.

Message Type

LOG

Message Severity

['MAPS-3008 : CRITICAL', 'MAPS-3009 : ERROR', 'MAPS-3010 : WARNING', 'MAPS-3011 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

Recommended Action

Reduce the chassis wide committed zone DB size to the recommended scalability limit. This can be achieved by reducing the zone DB configurations per logical switch.

MAPS-3016 to MAPS-3019

Message

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>, Quiet Time=<Quiet Time>.

Message Type

LOG

Message Severity

['MAPS-3016 : CRITICAL', 'MAPS-3017 : ERROR', 'MAPS-3018 : WARNING', 'MAPS-3019 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

Recommended Action

No action needed from the user.

MAPS-3020 to MAPS-3023

Message

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>, Quiet Time=<Quiet Time>.

Message Type

LOG

Message Severity

['MAPS-3020 : CRITICAL', 'MAPS-3021 : ERROR', 'MAPS-3022 : WARNING', 'MAPS-3023 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

Recommended Action

No action needed from the user.

MAPS-3024 to MAPS-3027

Message

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>, Quiet Time=<Quiet Time>.

Message Type

LOG

Message Severity

['MAPS-3024 : CRITICAL', 'MAPS-3025 : ERROR', 'MAPS-3026 : WARNING', 'MAPS-3027 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

Recommended Action

Verify that the location temperature is within the operational range of the switch. Refer to the hardware reference manual for the environmental temperature range of your switch. Execute the `fanShow` command to verify that all fans are running at normal speeds. If any fans are missing or not performing at a high enough speed, they should be replaced. Check the environment and ensure the room temperature is within the operational range of the switch. Ensure that there are no blockages of the airflow around the chassis. If temperature problem is isolated to PSU / FAN then reseal the PSU / FAN. If the problem persists, replace the unit. If problem is isolated to blade then reseal the blade. If the problem persists, replace the blade.

MAPS-3036 to MAPS-3039**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>, Quiet Time=<Quiet Time>.

Message Type

LOG

Message Severity

['MAPS-3036 : CRITICAL', 'MAPS-3037 : ERROR', 'MAPS-3038 : WARNING', 'MAPS-3039 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

Recommended Action

In case of E-Port Oversubscription, need to increase the ISL trunk ports and in case F-Port Oversubscription, need to upgrade the link to higher speed to match IO demands.

MAPS-3040 to MAPS-3043**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>, Quiet Time=<Quiet Time>.

Message Type

LOG

Message Severity

['MAPS-3040 : CRITICAL', 'MAPS-3041 : ERROR', 'MAPS-3042 : WARNING', 'MAPS-3043 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

Recommended Action

This indicates some SFP on the switch is in error state. Please check for SFP rule alerts and sfpshow command for more details. Replace problematic SFPs as per recommendation.

MAPS-3052 to MAPS-3055**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>, Quiet Time=<Quiet Time>.

Message Type

LOG

Message Severity

['MAPS-3052 : CRITICAL', 'MAPS-3053 : ERROR', 'MAPS-3054 : WARNING', 'MAPS-3055 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

Recommended Action

Access your switch vendor support portal to obtain and install a new Trusted FOS Certificate.

MAPS-3056 to MAPS-3059**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>, Quiet Time=<Quiet Time>.

Message Type

LOG

Message Severity

['MAPS-3056 : CRITICAL', 'MAPS-3057 : ERROR', 'MAPS-3058 : WARNING', 'MAPS-3059 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

Recommended Action

Access your switch vendor support portal to obtain and install a new Trusted FOS Certificate.

MAPS-3060 to MAPS-3063**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>, Quiet Time=<Quiet Time>.

Message Type

LOG

Message Severity

['MAPS-3060 : CRITICAL', 'MAPS-3061 : ERROR', 'MAPS-3062 : WARNING', 'MAPS-3063 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

Recommended Action

Verify connectivity from switch to Support Link Server (bsnconnect.broadcom.com) or ASC-Gateway if deployed. Suggested troubleshooting steps. 1. Verify DNS server is configured and reachable. 2. Verify the Support Link Server is reachable (ping bsnconnect.broadcom.com) or ASC-Gateway (ping ascg.domain.name). Retry upload with command supportlink --sendand check log for confirmation or error.

MAPS-3064 to MAPS-3067**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>, Quiet Time=<Quiet Time>.

Message Type

LOG

Message Severity

['MAPS-3064 : CRITICAL', 'MAPS-3065 : ERROR', 'MAPS-3066 : WARNING', 'MAPS-3067 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

Recommended Action

Outstanding IOs on Target exceeded threshold. This could happen due to various reasons like host/target mis-configuration, performance issues on the host/target devices, congestion in the fabric due to slow drain devices etc. Please check for other MAPS alerts related to port errors or credit stall issues.

MAPS-3068 to MAPS-3071**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>, Quiet Time=<Quiet Time>.

Message Type

LOG

Message Severity

['MAPS-3068 : CRITICAL', 'MAPS-3069 : ERROR', 'MAPS-3070 : WARNING', 'MAPS-3071 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

Recommended Action

Outstanding IOs on Target exceeded threshold. This could happen due to various reasons like host/target mis-configuration, performance issues on the host/target devices, congestion in the fabric due to slow drain devices etc. Please check for other MAPS alerts related to port errors or credit stall issues.

MAPS-3072 to MAPS-3075**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>, Quiet Time=<Quiet Time>.

Message Type

LOG

Message Severity

['MAPS-3072 : CRITICAL', 'MAPS-3073 : ERROR', 'MAPS-3074 : WARNING', 'MAPS-3075 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

Recommended Action

IO exchanges that are timing out has exceeded the configured threshold. This could happen due to various reasons like host/target mis-configuration, performance issues on the host/target devices, congestion in the fabric due to slow drain devices etc. Please check for other MAPS alerts related to port errors or credit stall issues.

MAPS-3088 to MAPS-3091**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>, Quiet Time=<Quiet Time>.

Message Type

LOG

Message Severity

['MAPS-3088 : CRITICAL', 'MAPS-3089 : ERROR', 'MAPS-3090 : WARNING', 'MAPS-3091 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

Recommended Action

IO exchanges that are errored out has exceeded the configured threshold. This could happen due to various reasons like host/target mis-configuration, performance issues on the host/target devices, congestion in the fabric due to slow drain devices etc. Please check for other MAPS alerts related to port errors or credit stall issues.

MAPS-3092 to MAPS-3095**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>, Quiet Time=<Quiet Time>.

Message Type

LOG

Message Severity

['MAPS-3092 : CRITICAL', 'MAPS-3093 : ERROR', 'MAPS-3094 : WARNING', 'MAPS-3095 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

Recommended Action

Outstanding IOs on Target exceeded threshold. This could happen due to various reasons like host/target mis-configuration, performance issues on the host/target devices, congestion in the fabric due to slow drain devices etc. Please check for other MAPS alerts related to port errors or credit stall issues.

MAPS-3096 to MAPS-3099**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>, Quiet Time=<Quiet Time>.

Message Type

LOG

Message Severity

['MAPS-3096 : CRITICAL', 'MAPS-3097 : ERROR', 'MAPS-3098 : WARNING', 'MAPS-3099 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

Recommended Action

Outstanding IOs on Target exceeded threshold. This could happen due to various reasons like host/target mis-configuration, performance issues on the host/target devices, congestion in the fabric due to slow drain devices etc. Please check for other MAPS alerts related to port errors or credit stall issues.

MAPS-3120 to MAPS-3123**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>, Quiet Time=<Quiet Time>.

Message Type

LOG

Message Severity

['MAPS-3120 : CRITICAL', 'MAPS-3121 : ERROR', 'MAPS-3122 : WARNING', 'MAPS-3123 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

Recommended Action

IO exchange first response from Target is taking more than configured threshold. This could happen due to various reasons like host/target mis-configuration, performance issues on the host/target devices, congestion in the fabric due to slow drain devices etc. Please check for other MAPS alerts related to port errors or credit stall issues.

MAPS-3124 to MAPS-3127**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>, Quiet Time=<Quiet Time>.

Message Type

LOG

Message Severity

['MAPS-3124 : CRITICAL', 'MAPS-3125 : ERROR', 'MAPS-3126 : WARNING', 'MAPS-3127 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

Recommended Action

IO exchange first response from Target is taking more than configured threshold. This could happen due to various reasons like host/target mis-configuration, performance issues on the host/target devices, congestion in the fabric due to slow drain devices etc. Please check for other MAPS alerts related to port errors or credit stall issues.

MAPS-3128 to MAPS-3131**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>, Quiet Time=<Quiet Time>.

Message Type

LOG

Message Severity

['MAPS-3128 : CRITICAL', 'MAPS-3129 : ERROR', 'MAPS-3130 : WARNING', 'MAPS-3131 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

Recommended Action

IO exchange completion is taking more than configured threshold. This could happen due to various reasons like host/target mis-configuration, performance issues on the host/target devices, congestion in the fabric due to slow drain devices etc. Please check for other MAPS alerts related to port errors or credit stall issues

MAPS-3132 to MAPS-3135**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>, Quiet Time=<Quiet Time>.

Message Type

LOG

Message Severity

['MAPS-3132 : CRITICAL', 'MAPS-3133 : ERROR', 'MAPS-3134 : WARNING', 'MAPS-3135 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

Recommended Action

IO exchange completion is taking more than configured threshold. This could happen due to various reasons like host/target mis-configuration, performance issues on the host/target devices, congestion in the fabric due to slow drain devices etc. Please check for other MAPS alerts related to port errors or credit stall issues

MAPS-3136 to MAPS-3139**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>, Quiet Time=<Quiet Time>.

Message Type

LOG

Message Severity

['MAPS-3136 : CRITICAL', 'MAPS-3137 : ERROR', 'MAPS-3138 : WARNING', 'MAPS-3139 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-3140 to MAPS-3143

Message

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>, Quiet Time=<Quiet Time>.

Message Type

LOG

Message Severity

['MAPS-3140 : CRITICAL', 'MAPS-3141 : ERROR', 'MAPS-3142 : WARNING', 'MAPS-3143 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

Recommended Action

Access your switch vendor support portal to obtain and install a new Trusted FOS Certificate.

MAPS-3144 to MAPS-3147

Message

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>, Quiet Time=<Quiet Time>.

Message Type

LOG

Message Severity

['MAPS-3144 : CRITICAL', 'MAPS-3145 : ERROR', 'MAPS-3146 : WARNING', 'MAPS-3147 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

Recommended Action

IO exchanges that are errored out has exceeded the configured threshold. This could happen due to various reasons like host/target mis-configuration, performance issues on the host/target devices, congestion in the fabric due to slow drain devices etc. Please check for other MAPS alerts related to port errors or credit stall issues.

MAPS-3148 to MAPS-3151

Message

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>, Quiet Time=<Quiet Time>.

Message Type

LOG

Message Severity

['MAPS-3148 : CRITICAL', 'MAPS-3149 : ERROR', 'MAPS-3150 : WARNING', 'MAPS-3151 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

Recommended Action

ITL reservation commands issued on that target has exceeded the configured threshold. This could cause performance issues for applications. Review the Initiator configuration to find reason for so many ITL reservation commands.

MAPS-3152 to MAPS-3155

Message

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>, Quiet Time=<Quiet Time>.

Message Type

LOG

Message Severity

['MAPS-3152 : CRITICAL', 'MAPS-3153 : ERROR', 'MAPS-3154 : WARNING', 'MAPS-3155 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-3156 to MAPS-3159

Message

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>, Quiet Time=<Quiet Time>.

Message Type

LOG

Message Severity

['MAPS-3156 : CRITICAL', 'MAPS-3157 : ERROR', 'MAPS-3158 : WARNING', 'MAPS-3159 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-3184 to MAPS-3187

Message

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>, Quiet Time=<Quiet Time>.

Message Type

LOG

Message Severity

['MAPS-3184 : CRITICAL', 'MAPS-3185 : ERROR', 'MAPS-3186 : WARNING', 'MAPS-3187 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-3188 to MAPS-3191

Message

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>, Quiet Time=<Quiet Time>.

Message Type

LOG

Message Severity

['MAPS-3188 : CRITICAL', 'MAPS-3189 : ERROR', 'MAPS-3190 : WARNING', 'MAPS-3191 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-3192 to MAPS-3195

Message

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>, Quiet Time=<Quiet Time>.

Message Type

LOG

Message Severity

['MAPS-3192 : CRITICAL', 'MAPS-3193 : ERROR', 'MAPS-3194 : WARNING', 'MAPS-3195 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-3196 to MAPS-3199**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>, Quiet Time=<Quiet Time>.

Message Type

LOG

Message Severity

['MAPS-3196 : CRITICAL', 'MAPS-3197 : ERROR', 'MAPS-3198 : WARNING', 'MAPS-3199 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-3200 to MAPS-3203**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>, Quiet Time=<Quiet Time>.

Message Type

LOG

Message Severity

['MAPS-3200 : CRITICAL', 'MAPS-3201 : ERROR', 'MAPS-3202 : WARNING', 'MAPS-3203 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MAPS-3204 to MAPS-3207**Message**

<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>, Quiet Time=<Quiet Time>.

Message Type

LOG

Message Severity

['MAPS-3204 : CRITICAL', 'MAPS-3205 : ERROR', 'MAPS-3206 : WARNING', 'MAPS-3207 : INFO']

Probable Cause

Indicates that the specified rule has been triggered because the errors are above the configured threshold.

MFIC Messages

MS-FICON error messages.

MFIC-1001**Message**

failure at sysmod_scn registry rc= <failure reason>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates the system is temporarily out of resources.

Recommended Action

No action is required; this message is often transitory.

If the message persists, run the `reboot` or the `haFailover` command (if applicable).

If the message persists, run the `supportFtp` command (as needed) to set up automatic FTP transfers; then run the `supportSave` command and contact your switch service provider.

MFIC-1002**Message**

Chassis FRU header not programmed for switch NID, using defaults (applies only to FICON environments).

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that custom switch node descriptor (NID) fields have not been programmed in nonvolatile storage. The default values are used. The Switch NID is used only in the following SB ELS frames: Request Node Identification Data (RNID) and Registered Link Incident Record (RLIR). The use of SB-3 link incident registration and reporting is typically limited to FICON environments.

Recommended Action

No action is required if SB-3 link incident registration and reporting is not used by the host or if default values are desired for the switch node descriptor fields.

MFIC-1003**Message**

Effective Insistent domain ID for the fabric changed from <state> to <state>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that one or more switches joined the fabric with an insistent domain ID (IDID) mode setting that is different from the current effective IDID mode for the fabric. This message also occurs when the IDID for the fabric has been turned on or off. The possible values for the state are "On" and "Off".

Recommended Action

IDID mode is a fabric-wide mode; make sure that any switches added to the fabric are configured with the same IDID mode as the fabric. If you are enabling or disabling IDID mode, this message is for information purposes only, and no action is required. IDID mode can be set using the `configure` command in the CLI or checking the Advanced Web Tools **Switch Admin > Configure > Fabric > Insistent Domain ID Mode** check box. The switch must be disabled to change the IDID mode.

MM Messages

Management modules error messages.

MM-1001**Message**

VPD block 0 CRC is bad.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the CRC in VPD block 0 is bad. This could indicate corruption or tampering.

Recommended Action

Execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

MPTH Messages

Management modules error messages.

MPTH-1003

Message

No minimum cost path in candidate list.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the fabric shortest path first (FSPF) module has determined that there is no minimum cost path (MPATH) available in the candidate list.

MQ Messages

Message queues error messages.

MQ-1004

Message

`mqRead`, queue = <queue name>, queue ID = <queue ID>, type = <message type>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates an unexpected message has been received in the specified message queue. The *queue name* value is always fspf_q. The *queue ID* and *message type* values can be any of the following:

- 2 - MSG_TX
- 3 - MSG_INTR
- 4 - MSG_STR
- 6 - MSG_ASYNC_IU
- 7 - MSG_LINIT_IU
- 8 - MSG_RSCN
- 9 - MSG_IOCTL
- 10 - MSG_ACCEPT
- 11 - MSG_IU_FREE
- 12 - MSG_US
- 13 - MSG_EXT_RSCN
- 14 - MSG_RDTS_START
- 15 - MSG_RDTS_SENDEFP
- 16 - MSG_RDTS_RESET

MQ-1005**Message**

queue <queue name>: queue full (miss=<miss count>).

Message Type

LOG | FFDC

Message Severity

WARNING

Probable Cause

Indicates that the specified message queue is full.

MQ-1006**Message**

queue <queue name>: msg too long (<number of bytes>:<message queue size>).

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates the incoming message size is larger than the message queue size.

MQ-1007**Message**

queue <queue name>: queue full (miss=<miss count>).

Message Type

LOG | FFDC

Message Severity

WARNING

Probable Cause

Indicates that the specified message queue is full.

MS Messages

Management Service (MS) error messages.

MS-1001**Message**

MS Platform Segmented port=<port number> (0x<port number (hex)>) (<reason for segmentation> <domain> (0x<domain (hex)>)).

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the Management Server (MS) has segmented from another switch domain at the specified port because of errors or inconsistencies defined in the MS platform service.

Recommended Action

Reboot or power cycle the switch.

MS-1002

Message

MS Platform Service Unstable(<message string><domain number>).

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the Management Server (MS) platform service is unstable.

The *message string* value can be one of the following:

- No Resp for GCAP from: The switch did not respond to a request for a GCAP (MS Get Capabilities) command.
- GCAP sup but not PL by: GCAP is supported but the flag for MS platform service is not set.
- GCAP Rejected (reason =BUSY) by: GCAP is not supported by another switch.
- Reject EXGPLDB from: The request to the exchange platform database was rejected. The remote switch may be busy.

The *domain number* is the target domain that caused the error.

Recommended Action

The recommended actions are as follows:

- No Resp for GCAP from: No action is required.
- GCAP sup but not PL by: Set the flag for the MS platform service.
- GCAP Rejected (reason =BUSY) by: Execute the `firmwareDownload` command to upgrade the firmware level on the switch to a level that supports reliable commit service (RCS).
- Reject EXGPLDB from: Wait a few minutes and try the command again.

MS-1003

Message

MS detected Unstable Fabric(<message string><domain number>).

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the Management Server (MS) detected an unstable fabric; the command or operation may not be successfully completed. This message is often transitory.

The *message string* value can be one of the following:

- DOMAIN_INVALID for a req from: The domain is invalid for a request.
- No WWN for: Unable to acquire the World Wide Name (WWN) for the corresponding domain.

The *domain number* is the target domain that caused error.

Recommended Action

The fabric may be reconfiguring, forming, or merging. Wait a few minutes and try the operation again.

Execute the `fabricShow` command or the `secFabricShow` command to verify that the number of domains matches the Management Server known domains.

If the message persists, execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

MS-1004

Message

MS detected ONLY 1 Domain(d=<domain in local resource>).

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the Management Server (MS) detected an unstable count of domains in its own local resource. This message is often transitory.

Recommended Action

The fabric may be reconfiguring, forming, or merging. Wait a few minutes and try the operation again.

Execute the `fabricShow` command or the `secFabricShow` command to verify that the number of domains matches the Management Server known domains.

If the message persists, execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

MS-1005

Message

MS Invalid CT Response from d=<domain>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the Management Server (MS) received an invalid common transport (CT) response from the switch domain. MS expects either a CT accept IU or a reject IU; the MS received neither response, which violates the Fibre Channel - Generic Services (FS-GS) specification.

Recommended Action

Check the integrity of the FC switch at the specified domain. It is not sending correct MS information as defined by the Fibre Channel - Framing and Signaling (FC-FS) standard.

MS-1006**Message**

MS Unexpected iu_data_sz=<number of bytes>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the Management Server (MS) received an information unit (IU) data of unexpected size. The IU payload and the IU size may be inconsistent with each other or with the command that is currently being processed.

Recommended Action

Wait a few minutes and try the operation again.

If the message persists, execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

MS-1008**Message**

MS Failure while initializing <action>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the Management Server (MS) failed while initializing the specified action. This message is often transitory.

The *action* can be one of the following:

- while writing to ms_els_q: MS is unable to write a message to the MS Extended Link Service Queue.
- while inserting timer to timer list: MS is unable to add a timer to a resource.

Recommended Action

If the error persists, check the available memory on the switch using the `memShow` command.

MS-1009**Message**

RLIR event. Slot/Port <slot number>/<port number> (0x<PID (hex)>). Device Port Tag is 0x<port tag>. <message text>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates a registered link incident record (RLIR) has been generated for one of the actions indicated by the *message* value.

The *message* value can be one of the following:

- Exceeded bit error rate threshold
- Loss of signal or synchronization
- Not operational seq recognized
- Primitive sequence timeout
- Unrecognized link incident

Recommended Action

Persistent RLIR incidents are likely the result of SAN hardware problems such as bad cables or small form-factor pluggable (SFP) transceivers. If the message persists, replace hardware.

MS-1021**Message**

MS WARMBOOT failure(<failure reason><failure reason code>).

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the Fabric OS state synchronization (FSS) warm recovery failed during the WARM INIT phase of a reboot.

Recommended Action

If the message persists, execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

MS-1022**Message**

Management Server Platform Service <Activated or Deactivated>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the Management Server (MS) platform service is being activated or deactivated.

MS-1023**Message**

Management Server Topology Discovery Service <Enabled or Disabled>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the Management Server (MS) topology discovery service is being enabled or disabled.

MS-1024**Message**

Management Server Access Control List is Updated.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the Management Server (MS) Access Control List (ACL) is saved to nonvolatile storage.

MS-1025**Message**

Possible Failover could have occurred while enabling MS Platform Service.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that a failover occurred when Management Server (MS) platform service was being enabled. This can leave the fabric in an inconsistent state.

Recommended Action

If any inconsistency in MS platform service exists within the fabric, enable MS platform service.

MS-1026**Message**

MS Platform disabled port <port number> domain <domain> to block enabling Platform service through merge operation.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the Management Server (MS) has disabled the specified E_Port connected to the specified domain because an implicit enable operation of the MS platform service has been blocked.

Recommended Action

Enable MS platform service on the switch and re-enable the port to join the fabric.

MS-1027**Message**

Fabric Name - <fabric_name> configured.

Message Type

AUDIT | LOG

Message Class

FABRIC

Message Severity

INFO

Probable Cause

Indicates that the specified fabric name is configured or renamed.

MS-1028**Message**

Fabric Name - <fabric_name> Cleared.

Message Type

AUDIT | LOG

Message Class

FABRIC

Message Severity

INFO

Probable Cause

Indicates that the specified fabric name is cleared.

MS-1029**Message**

Duplicate Fabric Name - <fabric_name> matching with FID <Fabric ID>.

Message Type

AUDIT | LOG

Message Class

FABRIC

Message Severity

ERROR

Probable Cause

Indicates that the configured fabric name is already used for another partition.

Recommended Action

Select a different fabric name and reconfigure.

MS-1030**Message**

Fabric Name - <fabric_name> <cmd> Failed for domain <domain>.

Message Type

AUDIT | LOG

Message Class

FABRIC

Message Severity

ERROR

Probable Cause

Indicates that fabric name configure or clear operation failed in Fibre Channel Router (FCR).

Recommended Action

Wait for fabric to stabilize and retry the operation.

MS-1031**Message**

Device 0x<device pid> queries QSA in a non FICON logical switch with HIF mode enabled.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that a FICON channel or device tries to login to non FICON LS with HIF mode enabled.

Recommended Action

If a FICON channel or device has to login, the logical switch should be converted to a FICON LS or the port should be moved to a FICON Logical Switch.

NBFS Messages

NBFS module error messages.

NBFS-1001

Message

Duplicate E_Port SCN from port <portnumber> in state <state change name> (<state change number>).

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates a duplicate E_Port state change notification (SCN) was reported. The neighbor finite state machine (NBFSM) states are as follows:

- 0 - Down
- 1 - Init
- 2 - Database Exchange
- 3 - Database Acknowledge Wait
- 4 - Database Wait
- 5 - Full

NBFS-1002

Message

Wrong input: <state name> to neighbor FSM, state <current state name>, port <portnumber>.

Message Type

FFDC | LOG

Message Severity

ERROR

Probable Cause

Indicates the wrong input was sent to the neighbor finite state machine (NBFSM). NBFSM states are as follows:

- 0 - Down
- 1 - Init
- 2 - Database Exchange
- 3 - Database Acknowledge Wait
- 4 - Database Wait
- 5 - Full

If this error occurs repeatedly, then there is a problem in the protocol implementation between two switches.

Recommended Action

Run the `nbrStateShow` command to check the neighbor state of the port listed in the message. If it is Full, then this message can safely be ignored. Otherwise, run the `portDisable` and `portEnable` commands to refresh the port.

NBFS-1003**Message**

DB_XMIT_SET flag not set in state <current state name>, input <state name>, port <portnumber>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates the database transmit set flag was not set for the specified input state on the specified port. Neighbor finite state machine (NBFSM) states are as follows:

- 0 - Down
- 1 - Init
- 2 - Database Exchange
- 3 - Database Acknowledge Wait
- 4 - Database Wait
- 5 - Full

Recommended Action

No action is required. The Fabric OS automatically recovers from this problem.

NBFS-1004

Message

Wrong input: <state name> to neighbor FSM, state <current state name>, port <portnumber>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates the wrong input was sent to the neighbor finite state machine (NBFSM). NBFSM states are as follows:

- 0 - Down
- 1 - Init
- 2 - Database Exchange
- 3 - Database Acknowledge Wait
- 4 - Database Wait
- 5 - Full

If this error occurs repeatedly, then there is a problem in the protocol implementation between two switches.

Recommended Action

Run the `nbrStateShow` command to check the neighbor state of the port listed in the message. If it is Full, then this message can safely be ignored. Otherwise, run the `portDisable` and `portEnable` commands to refresh the port.

NBFS-1005

Message

FSPF experiencing link issues on port <port string> in state <current state name> (<state change number>).

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that FSPF is experiencing issues with frames on the link leading to unexpected inputs being sent to the neighbor finite state machine (NBFSM). NBFSM states are as follows:

- 0 - Down
- 1 - Init
- 2 - Database Exchange
- 3 - Database Acknowledge Wait
- 4 - Database Wait
- 5 - Full

If this error occurs repeatedly, then there is a problem running the FSPF exchange and synchronization protocol between two switches across the identified link.

Recommended Action

Run the `nbrStateShow` command to check the neighbor state of the port listed in the message. If it is Full, then this message can safely be ignored. Otherwise, please check the `portStatsShow` command to see if there are errors on the link. If there are errors, consider running the D-Port Diagnostics tests on the link and/or consider replacing and faulty or bad equipment such as cables or optics.

NBFS-1006

Message

The FSPF Dead Timer for port <port string> expired, connected to domain <domain ID of neighbor as of last HLO message>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that FSPF is experiencing issues receiving HLO frames on the link, causing the link's dead timer to expire and the link's neighbor finite state machine (NBFSM) to drop out of the Full state.

Recommended Action

Please ensure that both neighboring switches of the link are operating normally.

If either switch has crashed, been rebooted, or delayed after an HA operation, ensure the switch and link return to a fully functional state so that traffic may resume.

Check the `portStatsShow` and `portErrShow` commands to see if there were errors on the link. Use the `nbrStateShow` and `interfaceShow` commands to see the current state of the neighbor finite state machine (NBFSM) for the link.

NS Messages

Name Server module error messages.

NS-1001

Message

The response for request 0x<CT command code> from remote switch 0x<Domain Id> is larger than the max frame size the remote switch can support.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the response payload exceeds the maximum frame size the remote switch can handle.

Recommended Action

Execute the `firmwareDownload` command to upgrade the remote switch with Fabric OS v4.3 or later, or Fabric OS v3.2 or later, as appropriate for the switch type, so that it can support GMI to handle frame fragmentation and reassembly.

You can also reduce the number of devices connected to the local switch.

NS-1002

Message

Remote switch 0x<Domain Id> has firmware revision lower than 2.2: <Firmware Revision 1st character><Firmware Revision 2nd character><Firmware Revision 3rd character><Firmware Revision 4th character> which is not supported.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the local switch cannot interact with the remote switch because of incompatible or obsolete firmware.

Recommended Action

Execute the `firmwareDownload` command to upgrade the remote switch to the latest level of firmware.

NS-1003

Message

Number of local devices <Current local device count>, exceeds the standby can support <Local device count that standby can support>, can't send update.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the Name Server on the standby control processor (CP) has a lower supported capability than the active CP because of different firmware versions running on the active and standby CPs. This means that the active and standby CPs are out of sync. Any execution of the `haFailover` or `firmwareDownload` commands will be disruptive.

Recommended Action

To avoid disruption of traffic in the event of an unplanned failover, schedule a firmware download so that the active and standby CPs have the same firmware version.

Reduce the local device count to follow the capability of the earliest version of firmware.

NS-1004

Message

Number of local devices <Current local device count>, exceeds the standby can support <Local device count that standby can support>, can't sync.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the Name Server on the standby control processor (CP) has a lower supported capability than the active CP because of different firmware versions running on the active and standby CPs. This means that the active and standby CPs are out of sync. Any execution of the `haFailover` or `firmwareDownload` commands will be disruptive.

Recommended Action

To avoid disruption of traffic in the event of an unplanned failover, schedule a firmware download so that the active and standby CPs have the same firmware version.

Reduce the local device count to follow the capability of the earliest version of firmware.

NS-1009

Message

NS has detected a device with Node WWN as zero, pid 0x<device PID>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that a device has logged in with node World Wide Node Name (WWNN) as zero. Brocade Network Advisor (BNA) will not show the port connectivity.

Recommended Action

Check the device that logged in. The device could be faulty.

NS-1010

Message

CSCTL mode enabled on port <csctlport> QoS zoning will be ignored for devices on this port.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that class-specific control (CS_CTL) mode has been enabled on the specified port that has devices as members of a quality of service (QoS) zone.

Recommended Action

Remove the CS_CTL configured devices from the QoS zone.

NS-1012

Message

Detected duplicate WWPN [<WWPN>] - devices removed with PID 0x<existing device PID> and 0x<new device PID>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the devices with the same World Wide Port Name (WWPN) have been removed from the Name Server database.

Recommended Action

Verify the device reported with duplicate WWPN.

NS-1013**Message**

SIM_PORT with WWPN[<WWPN>] creating duplicate condition with PID 0x<duplicate device PID>. Removed PID 0x<disabled device PID> and disabled port <disabled Port>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the SIM port that is causing the duplicate condition has been removed from the Name Server database and the port is disabled.

Recommended Action

Verify the device reported with duplicate World Wide Port Name (WWPN) and re-enable the port if necessary.

NS-1014**Message**

Domain Capability is not available for domain <Domain>. Rejoin this domain to the fabric. Reason Code <Reason Code>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that domain capability is unavailable for the specified domain.

Recommended Action

Remove and rejoin the specified domain to the fabric.

NS-1015**Message**

Failed to update client capability to ESS (Exchange Switch Support) after maximum number of retries - return code <Failed return code>. Failing sync dump to standby CP.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that Exchange Switch Support (ESS) is unable to update its capability. Failed to send the sync dump to standby control processor (CP).

Recommended Action

Verify that HA synchronization has failed using the `haShow` command. If HA synchronization has failed, execute the `haSyncStart` command on active CP to resynchronize the HA state.

NS-1016**Message**

Device <PID of quarantined device> has been quarantined. Standby CP does not support this feature, cannot send update.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the Name Server on the standby control processor (CP) has a lower supported capability than the active CP because of different firmware versions running on the active and standby CPs. This means that the active and standby CPs are out of sync. Any execution of the `haFailover` or `firmwareDownload` commands will be disruptive.

Recommended Action

To avoid disruption of traffic in the event of an unplanned failover, schedule a firmware download so that the active and standby CPs have the same firmware version.

Reduce the local device count to follow the capability of the earliest version of firmware.

NS-1017**Message**

<Local or Remote> Domain <Domain ID of slow drain device>, Port index <User Port Index of slow drain device>, All devices zoned with the slow drain device 0x<PID of slow drain device> have been quarantined.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that all the devices that are zoned with the slow drain device have been quarantined.

Recommended Action

To check all affected devices zoned to the slow drain device please use the CLI nszonemember.

NS-1018**Message**

<Local or Remote> Domain <Domain ID of slow drain device>, Port index <User Port Index of slow drain device>, All devices zoned with the slow drain device 0x<PID of slow drain device> have been unquarantined.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that all the devices that are zoned with the slow drain device have been unquarantined.

Recommended Action

To check all affected devices zoned to the slow drain device please use the CLI nszonemember.

NS-1020

Message

<AG-connected or Remote or Local> device 0x<PID of registered slow drain device> registered as Slow Drain is not enforced due to zoned port limit exceeded.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the AG-connected or Remote / Local device flagged for Severe Latency / Frame Loss could not be quarantined due to the zoned port count more than 32.

Recommended Action

Requires manual intervention to correct the slow drain condition.

NS-1021

Message

Local Domain <Domain ID of slow drain device>, Port index <User Port Index of slow drain device>, unzoned device 0x<PID of slow drain device> has been <quarantined or unquarantined>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that unzoned local device have been imarked as quarantined or unquarantined.

Recommended Action

To check all affected devices zoned to the slow drain device please use the CLI nszonemember.

NS-1022

Message

CSCTL mode enabled for port index <Port Index of the device zoned with slow drain device>, flow to device 0x<PID of slow drain device> cannot be quarantined.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that CSCTL mode is enabled so cannot be quarantined.

Recommended Action

To check all affected devices zoned to the slow drain device please use the CLI nszonemember.

NS-1023**Message**

Request for <request type> flow from device 0x<PID of device from which the flow is quarantined> to quarantined device 0x<PID of slow drain device> of <Local or Remote> domain <Domain ID of slow drain device> is not successful.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that quarantine / unquarantine request fail.

Recommended Action

To check all affected devices zoned to the slow drain device please use the CLI nszonemember.

NS-1024**Message**

Flow from device 0x<PID of device from which the flow is quarantined> to quarantined device 0x<PID of slow drain device> of <Local or Remote> domain <Domain ID of slow drain device> has been successfully quarantined.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the device that is zoned with the slow drain device have been quarantined.

Recommended Action

To check all affected devices zoned to the slow drain device please use the CLI nszonemember.

NS-1025**Message**

Flow from device 0x<PID of device from which the flow is quarantined> to quarantined device 0x<PID of slow drain device> of <Local or Remote> domain <Domain ID of slow drain device> has been successfully unquarantined.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the device that is zoned with the slow drain device have been unquarantined.

Recommended Action

To check all affected devices zoned to the slow drain device please use the CLI nszonemember.

NS-1026**Message**

<Local or Remote> domain <Domain ID of slow drain device>, port index <User Port Index of slow drain device>: A zoned device 0x<PID of slow drain device> has been quarantined.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that A zoned device has been marked as a slow drain device.

Recommended Action

To check all affected devices zoned to the slow drain device please use the CLI nszonemember.

NS-1027

Message

<Local or Remote> domain <Domain ID of slow drain device>, port index <User Port Index of slow drain device>: A zoned quarantined device 0x<PID of slow drain device> has been unquarantined.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that a zoned slow drain device has been unquarantined.

Recommended Action

To check all affected devices zoned to the slow drain device please use the CLI nszonemember.

LLDP Messages

LLDP error message.

LLDP-1000

Message

LLDP is enabled.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the link layer discovery protocol (LLDP) is enabled globally.

LLDP-1001

Message

LLDP is disabled.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the link layer discovery protocol (LLDP) is disabled globally.

LLDP-1002**Message**

LLDP global configuration is changed.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the link layer discovery protocol (LLDP) global configuration has been changed.

LLDP-1003**Message**

LLDP is enabled on interface <InterfaceName>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the link layer discovery protocol (LLDP) is enabled on the specified interface.

LLDP-1004**Message**

LLDP is disabled on interface <InterfaceName>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the link layer discovery protocol (LLDP) is disabled on the specified interface.

LLDP-1005**Message**

Using auto-sense on interface <InterfaceName> to update DCBX version.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the auto-sense feature is used to detect the Data Center Bridging eXchange (DCBX) version on the specified interface. The DCBX version field will be automatically updated between the Converged Enhanced Ethernet (CEE) version and the pre-CEE version depending on the link neighbor.

PDM Messages

Parity Data Manager (PDM) module error messages.

PDM-1001**Message**

Failed to parse the pdm config.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the Parity Data Manager (PDM) process could not parse the configuration file. This may be caused by a missing configuration file during the installation.

Recommended Action

Execute the `firmwareDownload` command to reinstall the firmware.

If the message persists, execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

PDM-1002

Message

ipclnit failed.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the Parity Data Manager (PDM) process could not initialize the inter-process communication (IPC) mechanism.

Recommended Action

If the message persists, execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

PDM-1003

Message

pdm [-d] -S <service> -s <instance>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that a syntax error occurred when trying to launch the Parity Data Manager (PDM) process.

Recommended Action

Execute the `firmwareDownload` command to reinstall the firmware.

If the message persists, execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

PDM-1004

Message

PDM memory shortage.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the Parity Data Manager (PDM) process ran out of memory.

Recommended Action

Reboot or power cycle the switch.

If the message persists, execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

PDM-1005

Message

FSS register failed.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the Parity Data Manager (PDM) failed to register with the Fabric OS synchronization service (FSS).

Recommended Action

Execute the `firmwareDownload` command to reinstall the firmware.

If the message persists, execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

PDM-1006

Message

Too many files in sync.conf.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the sync.conf configuration file contains too many entries.

Recommended Action

Execute the `firmwareDownload` command to reinstall the firmware.

If the message persists, execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

PDM-1007**Message**

File not created: <file name>. errno=<errno>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the Parity Data Manager (PDM) process failed to create the specified file.

Recommended Action

Execute the `firmwareDownload` command to reinstall the firmware.

If the message persists, execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

PDM-1008**Message**

Failed to get the number of U_Ports.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the Parity Data Manager (PDM) system call to getCfg failed.

Recommended Action

Execute the `firmwareDownload` command to reinstall the firmware.

If the message persists, execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

PDM-1009

Message

Can't update Port Config Data.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the Parity Data Manager (PDM) system call to setCfg failed.

Recommended Action

Execute the `firmwareDownload` command to reinstall the firmware.

If the message persists, execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

PDM-1010

Message

File open failed: <file name>, errno=<errno>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the Parity Data Manager (PDM) process could not open the specified file.

Recommended Action

Execute the `firmwareDownload` command to reinstall the firmware.

If the message persists, execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

PDM-1011**Message**

File read failed: <file name>, Length(read=<Number of character read>, expected=<Number of characters expected>),
errno=<errno returned by read>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the Parity Data Manager (PDM) process could not read data from the specified file.

Recommended Action

Execute the `firmwareDownload` command to reinstall the firmware.

If the message persists, execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

PDM-1012**Message**

File write failed: <file name>. Length(read=<Number of character read>, write=<Number of characters written>),
errno=<errno returned by write>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the Parity Data Manager (PDM) process could not write data to the specified file.

Recommended Action

Execute the `firmwareDownload` command to reinstall the firmware.

If the message persists, execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

PDM-1013**Message**

File empty: <File Name>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the switch configuration file `/etc/fabos/fabos.[0|1].conf` is empty.

Recommended Action

Execute the `firmwareDownload` command to reinstall the firmware.

If the message persists, execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

PDM-1014**Message**

Access sysmod failed.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates a system call to `sysMod` failed.

Recommended Action

Execute the `firmwareDownload` command to reinstall the firmware.

If the message persists, execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

PDM-1017

Message

System (<Error Code>): <Command>.

Message Type

FFDC | LOG

Message Severity

CRITICAL

Probable Cause

Indicates that the specified system call failed.

Recommended Action

Execute the `firmwareDownload` command to reinstall the firmware.

If the message persists, execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

PDM-1019

Message

File path or trigger too long.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that one line of the `pdm.conf` file is too long.

Recommended Action

Execute the `firmwareDownload` command to reinstall the firmware.

If the message persists, execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

PDM-1020

Message

Long path name (<Path>/<File Name>), Skip.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the specified file path name is too long. The maximum character limit is 49 characters.

Recommended Action

Use path names not exceeding 49 characters in length for the files to be replicated.

PDM-1021

Message

Failed to download area port map.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that a system call failed.

Recommended Action

Execute the `firmwareDownload` command to reinstall the firmware.

If the message persists, execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

PDM-1022

Message

The switch is configured only with IPv6 addresses.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the Parity Data Manager (PDM) cannot synchronize with its peer because the firmware does not support IPv6.

Recommended Action

Configure the local switch with IPv4 addresses.

PDM-1023**Message**

RADIUS is configured with IPv6 addresses.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the Parity Data Manager (PDM) cannot synchronize with its peer because the remote access dial-in user server (RADIUS) is configured with IPv6 addresses. IPv6 is not supported by older firmware.

Recommended Action

Configure RADIUS with IPv4 addresses.

PDM-1024**Message**

DNS is configured with IPv6 addresses.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the Parity Data Manager (PDM) cannot synchronize with its peer because the Domain Name Service (DNS) is configured with IPv6 addresses. IPv6 is not supported by older firmware.

Recommended Action

Configure DNS with IPv4 addresses.

PDM-1025

Message

LDAP is configured with IPv6 addresses.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the Parity Data Manager (PDM) cannot synchronize with its peer because the Lightweight Directory Access Protocol (LDAP) server is configured with IPv6 addresses. IPv6 is not supported by older firmware.

Recommended Action

Configure the LDAP server with IPv4 addresses.

PDM-1026

Message

User defined roles configured.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the Parity Data Manager (PDM) cannot synchronize with its peer because the user-defined roles are configured. User-defined roles are not supported by older firmware.

Recommended Action

Remove user-defined roles configuration.

PDM-1027

Message

Invalid port number: <port number> read from str: <str> for the LS: <sw_inst>

Message Type

LOG | FFDC

Message Severity

WARNING

Probable Cause

Indicates that the port number read from str is out of bounds.

Recommended Action

Continue with the next port number. Skip invalid port number before accessing list with port number as index.

PDM-1028

Message

Port cfg: b4[0] = 0x<first word> , b4[1] = 0x<second word>, b4[2] = 0x<third word>, b4[3] = 0x<fourth word>

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the port number read from str is out of bounds.

Recommended Action

Continue with the next port number. Skip invalid port number before accessing list with port number as index.

PDTR Messages

Panic dump trace files module error messages

PDTR-1001

Message

<informational message>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that information has been written to the panic dump files. The watchdog register codes are as follows:

- 0x10000000 - The watchdog timer (WDT) forced a core reset.
- 0x20000000 - The WDT forced a chip reset.
- All other code values are reserved.

Recommended Action

Run the `pdShow` command to view the panic dump and core dump files.

PDTR-1002**Message**

<informational message>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that information has been written to the panic dump and core dump files and a trap has been generated. The watchdog register codes are as follows:

- 0x10000000 - The watchdog timer (WDT) forced a core reset.
- 0x20000000 - The WDT forced a chip reset.
- All other code values are reserved.

Recommended Action

Run the `pdShow` command to view the panic dump and core dump files.

PLAT Messages

PLAT messages indicate hardware problems.

PLAT-1000**Message**

<Function name> <Error string>.

Message Type

FFDC | LOG

Message Severity

CRITICAL

Probable Cause

Indicates that nonrecoverable peripheral component interconnect (PCI) errors have been detected.

Recommended Action

The system will be faulted and may automatically reboot.

If the system does not reboot automatically, reboot the system manually using the `reboot` command.

Execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

PLAT-1001

Message

CP<Identifies which CP (0 or 1) is doing the reset> resetting other CP (double reset may occur).

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates the other control processor (CP) is being reset. This message is typically generated by a CP that is in the process of becoming the active CP. Note that in certain circumstances a CP may experience a double reset and reboot twice. A CP can recover automatically even if it has rebooted twice.

PLAT-1002

Message

CP<Identifies which CP (0 or 1) is generating the message>: <Error message> CP Fence 0x<CP Fence register. Contents (2 bytes) are platform-specific> 0x<CP Error register. Contents are platform-specific> CP Error 0x<Write control flag. Contents are platform-specific>.

Message Type

LOG

Message Severity

CRITICAL

Probable Cause

Indicates that the control processor (CP) cannot access the inter-integrated circuit (I2C) subsystem because of an error condition or because of being fenced or isolated from the I2C bus.

Recommended Action

Reboot the CP if it does not reboot automatically. Reseat the CP if rebooting does not solve the problem. If the problem persists, replace the CP.

PLAT-1003**Message**

<Info message> Slot <Blade Slot number> C/BE: 0x<Captured Command/Byte-Enables data> ADBUS: 0x<Captured AD bus data> misc_intr 0x<Bridge reset interrupts>.

Message Type

LOG | FFDC

Message Severity

CRITICAL

Probable Cause

Indicates that peripheral component interconnect (PCI) bus hang was detected.

Recommended Action

Replace the field-replaceable unit (FRU).

PLAT-1004**Message**

Active CP has older FPGA rev 0x<Older FPGA version major>_<Older FPGA version minor>. Upgrade to newer FPGA rev 0x<Newer FPGA version major>_<Newer FPGA version minor> .

Message Type

LOG | FFDC

Message Severity

CRITICAL

Probable Cause

Indicates that Fabric OS has older field-programmable gate array (FPGA) version. This message is applicable only to Brocade Gen6.

Recommended Action

Upgrade FPGA to new version.

PLAT-1005**Message**

Incompatible midplane detected. All internal ports will be disabled.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the chassis has a revision 1.0 midplane.

Recommended Action

Replace the midplane with a revision 1.1 midplane.

PLAT-1006**Message**

Unknown midplane revision.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the chassis has a midplane whose revision is unknown.

Recommended Action

Install newer firmware in the Chassis Management Controller (CMC).

PLAT-1007**Message**

BladeSystem Chassis type is unknown, setting maximum internal port speed to 8Gb/s.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the Onboard Administrator (OA) could be running an old version of firmware.

If OA firmware is new enough to support Enclosure Information, then the OA failed to send the Enclosure Information soon enough to allow the internal ports to run at 16GFC.

PLAT-1008**Message**

BladeSystem Enclosure Information arrived late from the OA.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the Onboard Administrator (OA) failed to send the Enclosure Information soon enough to allow the internal ports to run at 16GFC.

Recommended Action

Execute the `hareboot` command, followed by the `portdisable` and `portenable` commands, to allow internal ports to run at 16GFC.

PLAT-1009**Message**

BladeSystem Chassis type requires setting maximum internal port speed to 8Gb/s.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the chassis has an older midplane that cannot support 16GFC internal ports.

Recommended Action

Install the switch in a newer chassis.

PLAT-1010**Message**

SPDC HOST Initi failed spdc_status 0x<SPDC status register>, rdy0=0x<SPDC target ready register 0>, rdy1=0x<SPDC target ready register 1> fen=0x<fence register >, hk_fen=0x<hk_fence register >, ocp=0x<ocp_present register>.

Message Type

LOG | FFDC

Message Severity

CRITICAL

Probable Cause

Indicates that the Serial Private Data Channel (SPDC) host hardware encountered an unrecoverable error.

Recommended Action

Upgrade the control processor (CP) to the latest field-programmable gate array (FPGA) version, or replace the CP blade.

PLAT-1011**Message**

MAC signature 0x<Signature read> does not match.

Message Type

LOG | FFDC

Message Severity

CRITICAL

Probable Cause

Indicates that the MAC address cannot be read.

Recommended Action

The WWN card needs to be verified.

PLAT-1072

Message

The chassis is disabled because no Core Blades are available. Insert/replace one or both Core Blades and run `chassisenable`.

Message Type

FFDC | LOG

Message Severity

CRITICAL

Probable Cause

Indicates that the chassis has been disabled because of the unavailability of the core blades. There must be at least one core blade in enabled state for the chassis to be considered ready. All core blades are either missing, faulted, or powered off. This results in all logical switches (and ports) being disabled.

Recommended Action

Make sure that all core blade slots have core blades inserted and their ejector switches are closed. Power on core blades that are powered off, and power cycle or replace the core blades that are faulted.

Run the `chassisenable` command to re-enable the ports.

Running the `fastboot` or `reboot` command will also result in enabling the logical switches and ports.

PLAT-1073

Message

I2C read <VPD memory area> 0x<offset into the memory area> (bus addr 0x<i2c slave address>, mem addr 0x<EEPROM memory address>) len <requested data length>, i2c return <return value from lower level i2c function>, <formatted dump of first few bytes of data> reset_cnt <soft reset count> PID <process ID>

Message Type

FFDC | LOG

Message Severity

CRITICAL

Probable Cause**Recommended Action****PLAT-1100****Message**

Loss of AC source input detected on PS <PS number where AC source input loss was detected >.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the specified PS detected a loss of AC input.

Recommended Action

Perform an audit of the external AC source.

PLAT-2000**Message**

Hardware reset cause: first 0x<The first reset reason FPGA register value> - <The meaning of the first reset reason value>

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates the platform-specific source of the control processor (CP) reset. In the case of a rolling reboot, this value will indicate the platform-specific source of the first reset.

PLAT-2001**Message**

Hardware reset cause: latest: 0x<The latest reset reason FPGA register value> - <The meaning of the latest recent reset reason value>

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates the platform-specific source of the most recent control processor (CP) reset. In the case of a rolling reboot, this value will indicate the platform-specific source of the most recent reset.

PMGR Messages

A group of messages that relate to logical switch creation, deletion, and configuration.

PMGR-1001

Message

Attempt to create switch <FID> succeeded.

Message Type

LOG | AUDIT

Message Class

LS

Message Severity

INFO

Probable Cause

Indicates that the switch with the specified fabric ID (FID) was successfully created.

PMGR-1002

Message

Attempt to create switch <FID> failed. Error message: <Error Message>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the switch with the specified fabric ID (FID) was not created.

Recommended Action

Refer to the *Error Message* string displayed in the message for possible action.

PMGR-1003**Message**

Attempt to delete switch <FID> succeeded.

Message Type

LOG | AUDIT

Message Class

LS

Message Severity

INFO

Probable Cause

Indicates that the switch with the specified fabric ID (FID) was successfully deleted.

PMGR-1004**Message**

Attempt to delete switch <FID> failed. Error message: <Error Message>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the switch with the specified fabric ID (FID) was not deleted.

Recommended Action

Refer to the *Error Message* string displayed in the message for possible action.

PMGR-1005

Message

Attempt to move port(s) to switch <FID> succeeded.

Message Type

AUDIT | LOG

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates a successful attempt to move the ports to the specified switch.

PMGR-1006

Message

Attempt to move port(s) <Ports> on slot <Slot> to switch <FID> failed. Error message: <Error Message>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates an unsuccessful attempt to move the ports to the specified switch.

Recommended Action

Refer to the *Error Message* string displayed in the message for possible action.

PMGR-1007

Message

Attempt to change switch <FID> to switch <New FID> succeeded.

Message Type

AUDIT | LOG

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates successful change of the switch fabric ID (FID).

PMGR-1008**Message**

Attempt to change switch <FID> to switch <New FID> failed. Error message: <Error Message>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates a failed attempt to change the switch fabric ID (FID).

Recommended Action

Refer to the *Error Message* string displayed in the message for possible action.

PMGR-1009**Message**

Attempt to change the base switch to switch <FID> succeeded.

Message Type

AUDIT | LOG

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates successful change of the base switch.

PMGR-1010

Message

Attempt to change the base switch to switch <FID> failed. Error message: <Error Message>

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates a failed attempt to change the base switch.

Recommended Action

Refer to the *Error Message* string displayed in the message for possible action.

PMGR-1011

Message

Attempt to move port(s) to switch <FID> succeeded.

Message Type

AUDIT | LOG

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates a successful attempt to move the ports to the specified switch.

PMGR-1012

Message

Attempt to remove the base switch attribute from switch <FID> succeeded.

Message Type

AUDIT | LOG

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates successful removal of the base switch.

PMGR-1013

Message

Attempt to change the switch <FID> to ficon switch succeeded.

Message Type

AUDIT | LOG

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates successful change of switch into a FICON switch.

PMGR-1014

Message

Attempt to change the switch <FID> to a ficon switch failed. Error message: <Error Message>

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates a failed attempt to change a switch to FICON switch.

Recommended Action

Refer to the *Error Message* string displayed in the message for possible action.

PORT Messages

PORT module error messages.

PORT-1003

Message

Port <port number> Faulted because of many Link Failures.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates the specified port is now disabled because the link on this port had multiple failures that exceeded an internally set threshold on the port. This problem is typically related to hardware.

Recommended Action

Check and replace (if necessary) the hardware attached to both ends of the specified port number, including:

- The media (SFPs)
- The cable (fiber optic or copper inter-switch link (ISL))
- The attached devices

After checking the hardware, execute the `portEnable` command to re-enable the port.

PORT-1004

Message

Port <port number> (0x<port number (hex)>) could not be enabled because it is disabled due to long distance.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates the specified port is not enabled because other ports in the same group have used the buffers for this port group. This happens when other ports were configured to be long distance.

Recommended Action

To enable this port, perform one of the following actions:

- Reconfigure the other E_Ports so they are not long distance.
- Change the other E_Ports so they are not E_Ports.

This will free some buffers and allow this port to be enabled.

PORT-1005

Message

Slot <slot number> port <port on slot> does not support configured L_Port. Issue portCfgLport to clear configuration.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates the specified port is configured to be an L_Port, but the port does not support L_Port. If an L_Port is connected, then the port will be disabled because the port does not support L_Port. If an E_Port or F_Port is connected, then the port will not come up because it is configured to be an L_Port.

Recommended Action

Execute the `portCfgLport` command to clear the L_Port configuration.

PORT-1006

Message

Configuration changed for port (ID: <port number>) in No_Module or No_Light state.

Message Type

AUDIT | LOG

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates the configuration changes were made to an offline port in the No_Module or No_Light state.

PORT-1007

Message

Port (ID: <port number>) has been renamed to (<port name>).

Message Type

AUDIT | LOG

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates a port has been reconfigured with a different name.

PORT-1008

Message

GigE Port (<slot number>/GE<port number>) has been enabled.

Message Type

AUDIT | LOG

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates a Gigabit Ethernet port has been enabled of a particular slot.

PORT-1009

Message

GigE Port (<slot number>/GE<port number>) has been disabled.

Message Type

AUDIT | LOG

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates a Gigabit Ethernet port has been disabled of a particular slot.

PORT-1010**Message**

Port (ID: <port number>) QoS is disabled.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the port quality of service (QoS) is disabled due to the best effort setting on the 4Gb/s or 8Gb/s long distance platform.

PORT-1011**Message**

Please swap to the previous port blade, disable all F-Port trunk ports on this slot (<slot number>), and then swap back to current blade.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that port in the previous blade had F-port trunking enabled. The current port does not support F-Port trunking.

Recommended Action

Perform blade swap to the previous port blade, disable all F-Port trunk ports on this blade.

PORT-1012

Message

<Port name feature> has been removed for Port (ID: <Port number>).

Message Type

AUDIT | LOG

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that user configured port name or FICON-based port name has been removed for the specified port.

PORT-1013

Message

Port (ID: <port number>) is configured as Static D_Port.

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the port is configured as D_Port.

PORT-1014

Message

Port (ID: <port number>) is not configured as D_Port.

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the port is not configured as D_Port.

PORT-1015

Message

Port (ID: <Port number>) has been enabled.

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the port is being intentionally enabled.

PORT-1016

Message

Port (ID: <Port number>) has been disabled.

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the port is being intentionally disabled.

PORT-1017

Message

Port (ID: <Port number>) has been persistently enabled.

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the port is being persistently enabled.

PORT-1018

Message

Port (ID: <Port number>) has been persistently disabled.

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the port is being persistently disabled.

PORT-1019

Message

Default configuration update for port (ID: <Port number>).

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the specified port is updated with the default configuration.

PORT-1020**Message**

FEC configuration updated for port (ID: <Port number>).

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the specified port is updated with the Forward Error Correction (FEC) configuration.

PORT-1021**Message**

Long distance configuration updated for port (ID: <Port number>).

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the specified port is updated with the long distance configuration.

PORT-1022

Message

Octet speed combo configuration updated for port (ID: <Port number>).

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the specified port is updated with the octet speed combo configuration.

PORT-1023

Message

QOS configuration updated for port (ID: <Port number>).

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the specified port is updated with the quality of service (QoS) configuration.

PORT-1024

Message

Speed configuration updated for port (ID: <Port number>).

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the specified port is updated with the speed configuration.

PORT-1025**Message**

Trunk configuration updated for port (ID: <Port number>).

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the specified port is updated with the trunk configuration.

PORT-1026**Message**

ISL configuration updated for port (ID: <Port number>).

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the specified port is updated with the inter-switch link (ISL) configuration.

PORT-1027

Message

Port beacon configuration updated for port (ID: <Port number>).

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the specified port is updated with the port beacon configuration.

PORT-1028

Message

Portpeerbeacon configuration updated for port (ID: <Port number>).

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the specified port is updated with the portpeerbeacon configuration.

PORT-1029

Message

NPIV configuration updated for port (ID: <Port number>).

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the specified port is updated with the NPIV configuration.

PORT-1030**Message**

Compression configuration updated for port (ID: <Port number>).

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the specified port is updated with the Compression configuration.

PORT-1031**Message**

Encryption configuration updated for port (ID: <Port number>).

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the specified port is updated with the Encryption configuration.

PORT-1032

Message

TDZ configuration updated for port (ID: <Port number>).

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the specified port is updated with the TDZ configuration.

PORT-1033

Message

Non-DFE configuration updated for port (ID: <Port number>).

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the specified port is updated with the Non-DFE configuration.

PORT-1034

Message

Port statistics cleared for port (ID: <Port number>).

Message Type

AUDIT

Message Class

CLI

Message Severity

INFO

Probable Cause

Clears the statistics of the specified port.

PORT-1035

Message

Port (ID: <Port number>) has been configured as N-Port.

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the specified port is configured as N_Port.

PORT-1036

Message

Port (ID: <Port number>) is not configured as N_Port.

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the specified Port is not configured as N_Port.

PORT-1037

Message

Portcfgport configuration updated for port <Port Configuration>.

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the specified port is updated with the Portcfgport configuration.

PORT-1038

Message

port <Port number> is converted to <Flexport Configuration>.

Message Type

AUDIT

Message Class

CLI

Message Severity

INFO

Probable Cause

Indicates that the specified port is updated with the Portcfgflexport configuration.

PORT-1039

Message

Portcfgbreakout configuration for port <Port number> is <Breakout Configuration>.

Message Type

AUDIT

Message Class

CLI

Message Severity

INFO

Probable Cause

Indicates that the specified port is updated with the Portcfgbreakout configuration.

PORT-1040**Message**

Portcfggport configuration updated, <Configuration status> for port <Port number>.

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the specified port is either locked or released as G-Port.

PORT-1041**Message**

portCfgEportCredits configuration <Configuration status> for port <Port number>.

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates the credit allocation has been changed or restored for specified E/EX port.

PORT-1042

Message

ALPA(0x<ALPA>) configuration set for port <Port number>.

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates the ALPA has been changed or restored for specified port.

PORT-1043

Message

Credit recovery <Enabled or Disabled> for port <Port number>.

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates the credit recovery has been changed for specified port.

PORT-1044

Message

RSCN Suppressed configuration updated for port <Port number>.

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the specified port is updated with portcfggrscn configuration.

PORT-1045

Message

LOS TOV configuration updated for port <Port number>.

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates de-bouncing of signal loss for specified port has been changed using portcfglosstov.

PORT-1046

Message

Mirror port configuration updated for port <Port number>.

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the specified port is updated with the mirror port configuration.

PORT-1047

Message

SIM port configuration updated for port <Port number>.

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the specified port is updated with the SIM port configuration.

PORT-1048

Message

EX-port configuration updated for port <Port number>.

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the specified port is updated with the EX-port configuration.

PORT-1049

Message

Fault delay configuration updated for port <Port number>.

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the specified port is updated with the fault delay configuration.

PORT-1050**Message**

Port auto disable configuration updated for port <Port number>.

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the specified port is updated with the portcfgautodisable configuration.

PORT-1051**Message**

F_Port Buffers configuration updated for port <Port number>.

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the specified port is updated with the portcfgportbuffers configuration.

PORT-1052

Message

Port NPIV login limit is changed for port <Port number>.

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the specified port is updated with the Npiv login limit configuration.

PORT-1053

Message

FLOGI Logout capability updated for port <Port number>.

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the specified port is updated with the FLOGI Logout capability.

PORT-1054

Message

Port (ID: <Port number>) has been marked Impaired.

Message Type

AUDIT | LOG

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the port is being marked Impaired.

Recommended Action

Impaired links will not be used for routing unless no viable alternative exists without routing path cost changes.

Check and replace (if necessary) the hardware attached to both ends of the specified port number, including:

- The media (SFPs)
- The cable (fiber optic or copper inter-switch link (ISL))
- The attached devices

After checking the hardware, execute the `portRestart` to clear the Impaired state.

PORT-1055

Message

Port (ID: <Port number>) Impaired state has been cleared.

Message Type

AUDIT | LOG

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the port has cleared the Impaired state.

Recommended Action

The port must be toggled after clearing the Impaired state to return it to service.

PORT-1056

Message

Port (ID: <Port number>) Clean Address enabled.

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the port has clean address support enabled.

PORT-1057

Message

Port (ID: <Port number>) Clean Address disabled.

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the port has clean address support disabled.

PORT-1058

Message

<String> for port (ID: <Port number>).

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the ICL port has module inserted/removed.

PORT-1059

Message

Port (ID: <Port number>) Congestion detection signaling enabled.

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the port has congestion detection signaling enabled.

PORT-1060

Message

Port (ID: <Port number>) Congestion detection signaling disabled.

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the port has congestion detection signaling disabled.

PORT-1061

Message

Port (ID: <Port number>) user defined disable reason set.

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that user defined reason to disable the port has been set.

PORT-1062

Message

Port (ID: <Port number>) user defined disable reason cleared.

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that user defined reason to disable the port has been cleared.

PORT-1063

Message

Port (ID: <Port number>) Configured Application Server to No-Access.

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that user changed the Application Server access to no-access.

PORT-1064

Message

Port (ID: <Port number>) Configured Application Server to Read-Only.

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that user changed the Application Server access to read-only.

PORT-1065

Message

Port (ID: <Port number>) Configured Application Server to Read-Write.

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that user changed the Application Server access to read-write.

PORT-1066

Message

Port (ID: <Port number>) Configured Enhanced Fabric Configuration Server access to No-Access.

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that user changed the Enhanced Fabric Configuration Server access to no-access.

PORT-1067

Message

Port (ID: <Port number>) Configured Enhanced Fabric Configuration Server access to Read-Only.

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that user changed the Enhanced Fabric Configuration Server access to read-only.

PORT-1068

Message

Port (ID: <Port number>) Configured Enhanced Fabric Configuration Server access to Read-Write.

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that user changed the Enhanced Fabric Configuration Server access to read-write.

PORT-1069

Message

Port (ID: <Port number>) Configured Fabric Configuration Server access to No-Access.

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that user changed the Fabric Configuration Server access to no-access.

PORT-1070

Message

Port (ID: <Port number>) Configured Fabric Configuration Server access to Read-Only.

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that user changed the Fabric Configuration Server access to read-only.

PORT-1071

Message

Port (ID: <Port number>) Configured Fabric Configuration Server access to Read-Write.

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that user changed the Fabric Configuration Server access to read-write.

PORT-1072

Message

Port (ID: <Port number>) Configured Fabric Device Management Interface access to No-Access.

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that user changed the Fabric Device Management Interface access to no-access.

PORT-1073

Message

Port (ID: <Port number>) Configured Fabric Device Management Interface access to Read-Only.

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that user changed the Fabric Device Management Interface access to read-only.

PORT-1074

Message

Port (ID: <Port number>) Configured Fabric Device Management Interface access to Read-Write.

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that user changed the Fabric Device Management Interface access to read-write.

PORT-1075

Message

Port (ID: <Port number>) Configured Fabric Zone Server access to No-Access.

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that user changed the Fabric Zone Server access to no-access.

PORT-1076

Message

Port (ID: <Port number>) Configured Fabric Zone Server access to Read-Only.

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that user changed the Fabric Zone Server access to read-only.

PORT-1077**Message**

Port (ID: <Port number>) Configured Fabric Zone Server access to Read-Write.

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that user changed the Fabric Zone Server access to read-write.

PORT-1078**Message**

Port (ID: <Port number>) Configured Unzoned Name Server access to No-Access.

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that user changed the Unzoned Name Server access to no-access.

PORT-1079

Message

Port (ID: <Port number>) Configured Unzoned Name Server access to Read-Only.

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that user changed the Unzoned Name Server access to read-only.

PORT-1080

Message

port <User port> is connected to AG and Application Header configuration is enabled.

Message Type

LOG

Message Severity

INFO

Probable Cause

Application Header configuration is enabled for all AG-connected devices at the port.

PORT-1081

Message

SFP on Port:<Port number> programmed with new operating settings. R51(new:0x44, old:0x<Register R51 Old Value>), R56(new:0x99, old:0x<Register R56 Old Value>.)

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that SFP on the port has been programmed with new settings that provide increased link quality margin..

PORT-1082**Message**

portCfgAppHeader configuration <Configuration status> for port <Port number>.

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates the AppHeaderConfiguration is enabled or disabled for the specified port.

PS Messages

Performance Server daemon error messages.

PS-1000**Message**

Failed to initialize Advanced Performance Monitoring.

Message Type

FFDC | LOG

Message Severity

CRITICAL

Probable Cause

Indicates that an unexpected software error has occurred in Advanced Performance Monitoring. The Performance Monitor has failed to initialize.

Recommended Action

The control processor (CP) will reboot or failover automatically. If it does not, reboot or power cycle the switch to reinitiate the firmware.

PS-1001**Message**

Advanced Performance Monitoring configuration updated due to change in PID format.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the port ID (PID) format was changed.

Recommended Action

No action is required. Refer to the *Fabric OS Administrator's Guide* for more information about the PID format.

PS-1002**Message**

Failed to initialize the tracing system for Advanced Performance Monitoring.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that an unexpected software error has occurred in Advanced Performance Monitoring. The Performance Monitor tracing system has failed to initialize.

Recommended Action

Tracing will not be available for Advanced Performance Monitoring, but other functions will function normally. To activate tracing, reboot or failover the control processor (CP).

PS-1009

Message

Failed to add the device updates in condb database.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the fabric has more than the allowed number of devices.

Recommended Action

Reduce the number of devices configured in the fabric to be within the allowed limit. The maximum number of devices that can be configured in a fabric is 940.

PSWP Messages

Portswap module error messages.

PSWP-1001

Message

PID for port <wwn name corresponding to source port> and port <wwn name corresponding to destination port> are swapped. New PID for port <wwn name corresponding to source port> is 0x<wwn name corresponding to destination port> and port <new area corresponding to source wwn> is 0x<new area corresponding to destination wwn>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates the `portSwap` command has been issued.

PSWP-1002

Message

Port Swap feature enabled.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates the port swap feature has been enabled in the switch.

PSWP-1003**Message**

Port Swap feature disabled.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates the port swap feature has been disabled in the switch.

PSWP-1004**Message**

Blade Swap complete for slots <slot number corresponding to the source blade> and <slot number corresponding to the destination blade>.

Message Type

AUDIT | LOG

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates the `bladeSwap` command has been issued.

PSWP-1005

Message

Blade Swap undo failed with error code <error code from undoBladeSwap>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates the `bladeSwap` command has not been undone.

Recommended Action

Use the `portSwapShow` command to display a list of currently swapped ports; then use the `portSwap` command to achieve the desired result.

PSWP-1006

Message

Blade Swap failed on configInit with error code <error code from configInit> in switch number <current switch number>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates the `bladeSwap` command failed on access to configuration data.

Recommended Action

Retry the command. If the failure persists, contact your switch service provider.

PSWP-1007

Message

Blade Swap failed on fabosInit with error code <error code from fabosInit> in switch number <current switch number>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates the `bladeSwap` command failed on access to switch context.

Recommended Action

Retry the command. If the failure persists, contact your switch service provider.

PSWP-1008

Message

PID for port <source port> and port <destination port> are swapped.

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates the `portSwap` command has been issued.

RAS Messages

Informational messages when First Failure Data Capture (FFDC) events are logged to the FFDC log or when there is a roll-over warning.

RAS-1001

Message

First failure data capture (FFDC) event occurred.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that a first failure data capture (FFDC) event occurred and the failure data has been captured.

Recommended Action

Execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

RAS-1002**Message**

First failure data capture (FFDC) reached maximum storage size (<log size limit> MB).

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the storage size for first failure data capture (FFDC) has reached the maximum.

Recommended Action

Execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

RAS-1003**Message**

Tracedump transfer failed because anonymous FTP is not allowed when secure upload/download is set in `configurechassis`

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates support ftp parameters are set to user: anonymous, and password: BLANK when secure upload/download is set in `configurechassis`

Recommended Action

Change the support ftp parameters

RAS-1004

Message

Software 'verify' error detected.

Message Type

LOG | FFDC

Message Severity

INFO

Probable Cause

Indicates an internal software error.

Recommended Action

Execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

RAS-1005

Message

Software 'assert' error detected.

Message Type

LOG | FFDC

Message Severity

WARNING

Probable Cause

Indicates an internal software error.

Recommended Action

Execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

RAS-1006

Message

Support data file (<Uploaded file name>) automatically transferred to remote address ' <Remote target designated by user> '.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the support data was automatically transferred from the switch to the configured remote server.

RAS-1007

Message

System is about to reload.

Message Type

LOG | AUDIT

Message Class

CLI

Message Severity

INFO

Probable Cause

Indicates that the system reload was initiated.

RAS-1008

Message

supportftp parameters are not configured. One of the required parameter is missing.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that one or more support FTP parameters were not specified with the `supportFtp` command in non-interactive mode.

Recommended Action

Specify all support FTP parameters.

RAS-1009**Message**

Trace FTP is set to Host <Host Name> user: <User Name> remoteDir <File Path>

Message Type

AUDIT

Message Class

RAS

Message Severity

INFO

Probable Cause

Indicates trace ftp parameters are set.

RAS-1010**Message**

Trace FTP is set to <trace_ftp_enable success>

Message Type

AUDIT

Message Class

RAS

Message Severity

INFO

Probable Cause

Indicates trace ftp is enabled or disabled.

RAS-1011**Message**

<trace_dump_all success>

Message Type

AUDIT

Message Class

RAS

Message Severity

INFO

Probable Cause

Indicates tracedump is generated or not.

RAS-1012

Message

<trace_ftp_dump success or not>

Message Type

AUDIT

Message Class

RAS

Message Severity

INFO

Probable Cause

Indicates tracedump transferred to remote location is successful or not.

RAS-1013

Message

<trace_dump_remove>

Message Type

AUDIT

Message Class

RAS

Message Severity

INFO

Probable Cause

Indicates trace dump removed on a slot or not.

RAS-1014**Message**

<trace_trigger_remove_all>

Message Type

AUDIT

Message Class

RAS

Message Severity

INFO

Probable Cause

Indicates trace_trigger_remove_all is successful or not.

RAS-1015**Message**

<trace_trigger_remove>

Message Type

AUDIT

Message Class

RAS

Message Severity

INFO

Probable Cause

Indicates trace trigger is removed or not.

RAS-1016**Message**

<trace_trigger_set>

Message Type

AUDIT

Message Class

RAS

Message Severity

INFO

Probable Cause

Indicates trace trigger is set or not.

RAS-2001

Message

Audit message log is enabled.

Message Type

LOG | AUDIT

Message Class

RAS

Message Severity

INFO

Probable Cause

Indicates that the audit message log has been enabled.

RAS-2002

Message

Audit message log is disabled.

Message Type

LOG | AUDIT

Message Class

RAS

Message Severity

INFO

Probable Cause

Indicates that the audit message log has been disabled.

RAS-2003**Message**

Audit message class configuration has been changed to <New audit class configuration>.

Message Type

LOG | AUDIT

Message Class

RAS

Message Severity

INFO

Probable Cause

Indicates that the audit event class configuration has been changed.

RAS-2004**Message**

prom access is enabled.

Message Type

LOG | AUDIT

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates that the PROM access has been enabled.

RAS-2005**Message**

prom access is disabled.

Message Type

LOG | AUDIT

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates that the PROM access has been disabled.

RAS-2006

Message

Syslog server IP address <IP address> added.

Message Type

AUDIT

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates that a syslog server IP address has been added.

RAS-2007

Message

Syslog server IP address <IP address> removed.

Message Type

AUDIT

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates that a syslog server IP address has been removed.

RAS-2008**Message**

Audit log message storage has wrapped around.

Message Type

LOG | AUDIT

Message Class

RAS

Message Severity

INFO

Probable Cause

Indicates that audit log message storage has wrapped around.

RAS-2009**Message**

Audit log message storage has reached 75 percentage of limit.

Message Type

LOG | AUDIT

Message Class

RAS

Message Severity

INFO

Probable Cause

Indicates that audit log message storage is 75% full.

RAS-2010**Message**

Syslog daemon is started.

Message Type

AUDIT

Message Class

RAS

Message Severity

INFO

Probable Cause

Indicates that a syslog daemon is started.

RAS-2011

Message

Syslog daemon is stopped.

Message Type

AUDIT

Message Class

RAS

Message Severity

INFO

Probable Cause

Indicates that a syslog daemon is stopped.

RAS-2012

Message

Audit message severity configuration has been changed to <New audit severity configuration>.

Message Type

LOG | AUDIT

Message Class

RAS

Message Severity

INFO

Probable Cause

Indicates that the audit event severity configuration has been changed.

RAS-2013**Message**

syslog facility level has been changed from <Old syslog facility configuration> to <New syslog facility configuration>.

Message Type

LOG | AUDIT

Message Class

RAS

Message Severity

INFO

Probable Cause

Indicates that syslog facility configuration has been changed.

RAS-2014**Message**

Audit Log message <Audit Log message that has been disabled> has been disabled.

Message Type

LOG | AUDIT

Message Class

RAS

Message Severity

INFO

Probable Cause

Indicates that the specified Audit message has been disabled from logging.

RAS-2015**Message**

Audit Log message <Audit Log message that has been enabled> has been enabled.

Message Type

LOG | AUDIT

Message Class

RAS

Message Severity

INFO

Probable Cause

Indicates that the specified Audit message has been enabled for logging.

RAS-3001

Message

USB storage device plug-in detected.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the USB storage device plug-in has been detected.

RAS-3002

Message

USB storage device enabled.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the USB storage device has been enabled.

RAS-3003

Message

USB storage device was unplugged before it was disabled.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the USB storage device was unplugged before it was disabled.

Recommended Action

No action is required. It is recommended to disable the USB storage device using the `usbstorage -d` command before unplugged it from the system.

RAS-3004

Message

USB storage device disabled.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the USB storage device has been disabled.

RAS-3005

Message

CLI: <CLI command>

Message Type

AUDIT

Message Class

CLI

Message Severity

INFO

Probable Cause

Indicates that the specified command was executed on console.

RAS-3006**Message**

USB storage device enabled.

Message Type

AUDIT

Message Class

CLI

Message Severity

INFO

Probable Cause

Indicates that the USB storage device has been enabled.

RAS-3007**Message**

USB storage device disabled.

Message Type

AUDIT

Message Class

CLI

Message Severity

INFO

Probable Cause

Indicates that the USB storage device has been disabled.

RAS-3008

Message

USB storage <Storage file > removed.

Message Type

AUDIT

Message Class

CLI

Message Severity

INFO

Probable Cause

Indicates that the USB storage file has been removed.

RAS-3009

Message

The command <Command name> exits with return code: <return error code>. Message: <error string>

Message Type

AUDIT | LOG

Message Class

CLI

Message Severity

INFO

Probable Cause

Indicates that the `Command name` command exits with error code. The *error string* value indicates the reason for success/failure.

Recommended Action

Run the corresponding status related command for more information.

RCS Messages

Reliable Commit Service daemon module error messages.

RCS-1001

Message

RCS has been disabled. There was a problem verifying that all switches in the fabric support this feature.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the reliable commit service (RCS) feature has been disabled on the local switch because of problem validating RCS support on all switches in the fabric.

RCS is supported on all supported versions of Fabric OS. Indicates a possible routing problem.

Recommended Action

Run the `rcsInfoShow` command to view RCS capability on the fabric to determine problem switch or switches

RCS-1002

Message

RCS has been enabled.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the reliable commit service (RCS) feature has been enabled. RCS must be capable on all switches in the fabric to be enabled. If all switches are capable, it is automatically enabled.

RCS-1003

Message

Failed to allocate memory: (<function name>).

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the specified reliable commit service (RCS) function has failed to allocate memory.

Recommended Action

This message is usually transitory. Wait for few minutes and retry the command.

Check memory usage on the switch using the `memShow` command.

Reboot or power cycle the switch.

RCS-1004**Message**

Application(<application name>) not registered.<error string>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the specified application did not register with reliable commit service (RCS).

RCS is supported in Fabric OS v2.6, v3.1, v4.1 and later.

Recommended Action

Run the `haShow` command to view the HA state.

Run the `haDisable` and `haEnable` commands.

Run the `rscInfoShow` command to view RCS capability on the fabric. RCS is supported in Fabric OS v2.6, v3.1 and later, and v4.1 and later.

Run the `firmwareDownload` command to upgrade the firmware for any switches that do not support RCS.

RCS-1005**Message**

Phase <RCS phase>, <Application Name> Application returned <Reject reason>, 0x<Reject code>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that a receiving switch is rejecting the specified reliable commit service (RCS) phase.

Recommended Action

If the reject is in the acquire change authorization (ACA) phase, wait for several minutes and then retry the operation from the sender switch.

If the reject is in the stage fabric configuration (SFC) phase, check if the application license exists for the local domain and if the application data is compatible.

RCS-1006**Message**

State <RCS phase>, Application <Application Name> AD<Administrative Domain>, RCS CM. Domain <Domain ID that sent the reject> returned 0x<Reject code>. App Response Code <Application Response Code>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the specified domain rejected a reliable commit service (RCS) phase initiated by an application on the local switch.

- If the reject phase is acquire change authorization (ACA), the remote domain may be busy and could not process the new request.
- If the reject phase is stage fabric configuration (SFC), the data sent by the application may not be compatible or the domain does not have the license to support that application.

Recommended Action

If the reject is in the ACA phase, wait for several minutes and then retry the operation.

If the reject is in the SFC phase, check if the application license exists for the remote domain and if the application data is compatible.

RCS-1007**Message**

Zone DB size and propagation overhead exceeds domain <domain number>'s maximum supported Zone DB size <max zone db size>. Retry after reducing Zone DB size.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the specified domain cannot handle the zone database being committed.

Recommended Action

Reduce the zone database size.

RCS-1008

Message

Domain <domain number> Lowest Max Zone DB size.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates the specified domain has the lowest memory available for the zone database in the fabric. The zone database must be smaller than the memory available on this domain.

Recommended Action

Reduce the zone database size.

RCS-1009

Message

Request remote domain <domain number> offline because it does not support RCS.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the specified remote domain is requested to go offline to take it out of the fabric because it does not support reliable commit service (RCS).

Recommended Action

Run the `fabricShow` command to verify that the remote domain is out of the fabric.

RCS-1011**Message**

Remote domain <domain number> RCS-Validation message exchange Failed, Investigate frame delivery problem.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that for the specified domain, the RCS-capable information could not be retrieved due to some potential routing issues.

Recommended Action

Investigate for routing issue or check the cabling.

RCS-1012**Message**

Local domain is RCS incapable (ForceDisabled is <Flag which denotes whether switch is RCS capable or not>), hence reject the RCS_INFO request from domain <domain number>.

Message Type

LOG | FFDC

Message Severity

WARNING

Probable Cause

Indicates that the specified domain is RCS-incapable.

Recommended Action

Execute the `supportSave` command and contact your switch service provider.

RCS-1013

Message

Remote domain <domain number> is RCS incapable.

Message Type

LOG | FFDC

Message Severity

WARNING

Probable Cause

Indicates that the specified remote domain is RCS-incapable.

Recommended Action

Execute the `supportSave` command and contact your switch service provider.

RCS-1014

Message

Rebooting the CP as it received an update before application [<App Code>] has registered.

Message Type

LOG | FFDC

Message Severity

WARNING

Probable Cause

Indicates that the RCS in the control processor (CP) received an update before the application has registered. The CP reboots automatically to ensure sync and attain the normal state. This is a rare occurrence.

RPCD Messages

Remote Procedure Call daemon (RPCD) error messages.

RPCD-1001

Message

Authentication Error: client \"<IP address>\" has bad credentials: <bad user name and password pair>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates an authentication error was reported. The specified client IP address has faulty credentials.

Recommended Action

Enter the correct user name and password from the Fabric Access API host.

RPCD-1002**Message**

Missing certificate file. Secure RPCd is disabled.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates a Secure Sockets Layer (SSL) certificate is missing.

Recommended Action

To enable remote procedure call daemon (RPCD) in secure mode, install a valid SSL certificate on the switch.

RPCD-1003**Message**

Permission denied accessing certificate file. Secure RPCd is disabled.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates the Secure Sockets Layer (SSL) certificate file configured on the switch could not be accessed because root did not have read-level access.

Recommended Action

Change the file system access level for the certificate file to have root read-level access.

RPCD-1004**Message**

Invalid certificate file. Secure RPCd is disabled.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates the Secure Sockets Layer (SSL) certificate file has been corrupted.

Recommended Action

To enable remote procedure call daemon (RPCD) in secure mode, install a valid SSL certificate on the switch.

RPCD-1005**Message**

Missing private key file. Secure RPCd is disabled.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates the private key file is missing.

Recommended Action

Run the `secCertUtil` command to install a valid private key file.

RPCD-1006**Message**

Permission denied accessing private key file. Secure RPCd is disabled.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates the private key file configured on the switch could not be accessed because the root did not have read-level access.

Recommended Action

Change the file system access level for the private key file to have root read-level access.

RPCD-1007

Message

Invalid private file. Secure RPCd is disabled.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates the private key file has been corrupted.

Recommended Action

Run the `secCertUtil` command to install a valid private key file.

RTE Messages

RTE module error messages.

RTE-1001

Message

Detected route inconsistency. It may cause connectivity issues. If such issues arise, bounce all ISLs and ICLs on this chassis.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the constraints that are used to determine the paths for Dynamic Path Selection (DPS) are not synchronized from active control processor (CP) to standby CP during the failover. This event causes route inconsistencies.

Recommended Action

Reset all E_ports on the chassis using the `portDisable` and `portEnable` commands.

RTE-1002**Message**

FID <fid>: The QSFP connection topology is not recommended

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the current QSFP connection is resulting in an unbalanced topology and is not recommended.

Recommended Action

Use the `switchShow`, `islShow`, and `lsdbShow` commands to identify the QSFP connectivity to ensure that all recommendations for cabling are satisfied.

RTE-1003**Message**

FID <fid>: The QSFP connection topology has been corrected

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the previously unbalanced QSFP connection topology has been corrected.

RTE-1004

Message

Faulting blade <Slot number> due to missing routes. Use slotpoweroff and slotpoweron to recover the blade.

Message Type

LOG

Message Severity

WARNING

Probable Cause

The detection of a missing route suggests that more missing routes may exist. The blade is faulted in order to not impact the rest of the system.

Recommended Action

Run the commands `slotpoweroff` and `slotpoweron` to recover the blade.

RTE-1005

Message

Missing routes detected on slot <Slot number> but blade object 0x<blade object identifier> does not exist, so cannot recover.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Possible reasons for this raslog: the Interface Database(IFDB) is corrupted, out of sync, or missing data; or the slot may be in transition.

Recommended Action

Try manually running `slotpoweroff` and then `slotpoweron` with the slot number identified in the RASLOG text.

RTWR Messages

Reliable Transmit With Response service module error messages.

RTWR-1001

Message

RTWR <routine: error message> 0x<detail 1>, 0x<detail 2>, 0x<detail 3>, 0x<detail 4>, 0x<detail 5>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that an error occurred in Reliable Transport With Response (RTWR) due to one of the following reasons:

- The system ran out of memory.
- The domain may be unreachable
- The frame transmission failed.
- An internal error or failure occurred.

The message contains the name of the routine that has an error and other error-specific information. Refer to values in details 1 through 5 for more information.

Recommended Action

Restart the switch.

RTWR-1002

Message

RTWR <error message: maximum retries exhausted> 0x<port>, 0x<domain ID>, 0x<retry count>, 0x<status>, 0x<process ID>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that Reliable Transport With Response (RTWR) has exhausted the maximum number of retries for sending data to the specified domain.

Recommended Action

Execute the `fabricShow` command to verify that the specified domain ID is online.

If the switch with the specified domain ID is offline, enable the switch using the `switchEnable` command.

If the message persists, execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

RTWR-1003

Message

<module name>: RTWR retry <number of times retried> to domain <domain ID>, iu_data <first word of iu_data>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates the number of times Reliable Transport With Response (RTWR) has failed to get a response and retried.

Recommended Action

Execute the `fabricShow` command to verify that the specified domain ID is reachable.

If the message persists, execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

RTWR-1004

Message

RTWR <routine: error message> <Switch instance>, 0x<detail 1>, 0x<detail 2>, 0x<detail 3>.

Message Type

LOG | FFDC

Message Severity

ERROR

Probable Cause

Indicates that an error occurred in Reliable Transport With Response (RTWR)

The message contains the name of the routine that has an error and other error-specific information.

Recommended Action

Collect Support Save

SCN Messages

State Change Notification daemon error messages.

SCN-1001

Message

SCN queue overflow for process <daemon name>.

Message Type

FFDC | LOG

Message Severity

CRITICAL

Probable Cause

Indicates that an attempt to write a state change notification (SCN) message to a specific queue has failed because the SCN queue for the specified daemon is full. This may be caused by the daemon hanging or the system being busy.

The following are some valid values for the *daemon name*:

- fabricd
- asd
- evmd
- fcpd
- msd
- nsd
- psd
- snmpd
- zoned
- fspfd
- tsd

Recommended Action

If this message is caused by the system being busy, the condition is temporary.

If this message is caused by a hung daemon, the software watchdog will cause the daemon to dump the core and reboot the switch. In this case, execute the `supportSave` command to send the core files using FTP to a secure server location.

If the message persists, execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

SCN-1002

Message

SCN queue overflow for process <daemon name>.

Message Type

FFDC | LOG

Message Severity

WARNING

Probable Cause

Indicates that an attempt to write a state change notification (SCN) message to a specific queue has failed because the SCN queue for the specified daemon is full. This may be caused by the daemon hanging or the system being busy.

The following are some of the valid values for the *daemon name*:

- fabricd
- asd
- evmd
- fcpd
- msd
- nsd
- psd
- snmpd
- zoned
- fspfd
- tsd

Recommended Action

If this message is caused by the system being busy, the condition is temporary.

If this message is caused by a hung daemon, the software watchdog will cause the daemon to dump the core and reboot the switch. In this case, execute the `supportSave` command to send the core files using FTP to a secure server location.

If the message persists, execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

SEC Messages

Security daemon module error messages.

SEC-1001

Message

RCS process fails: <reason code>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the reliable commit service (RCS) process failed to complete. RCS is a mechanism for transferring data from one switch to other switches within the fabric. RCS ensures that either all or none of the switches commit to the database. RCS can fail if one switch in the fabric is busy or in an error state that prevents it from accepting the database.

RCS must be capable on all switches in the fabric to be enabled. If all switches are capable, it is automatically enabled.

Recommended Action

RCS is evoked when the security database is modified by a security command (for example, `secPolicySave`, `secPolicyActivate`, or `distribute`). If the switch is busy, the command may fail the first time. Retry the command.

If the message persists, execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

SEC-1002**Message**

Security data fails: <Reason Text>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the receiving switch fails to validate the security database sent from the primary fabric configuration server (FCS) switch. This may be caused by several factors: the data package may be corrupted, the time stamp on the package may be out of range as a result of replay attack or out-of-sync time service, or the signature verification failed. Signature verification failure may result from an internal error, such as losing the primary public key or an invalid database.

Recommended Action

Run the `secFabricShow` command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database may not be correctly updated for that switch. The error may also be a result of an internal corruption or a hacker attack to the secure fabric. If you have reason to believe that the error is the result of a possible security breach, take appropriate action as defined by your enterprise security policy.

SEC-1003**Message**

Fail to download security data to domain <Domain number> after <Number of retries> retries.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates the specified domain failed to download security data after the specified number of attempts, and that the failed switch encountered an error accepting the database download. The primary switch will segment the failed switch after 30 tries.

Recommended Action

Run the `secFabricShow` command to verify that the fabric is still consistent. All the switches should be in the ready state.

If the message persists, execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

SEC-1005**Message**

Primary FCS receives data request from domain <Domain number>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates the primary fabric configuration server (FCS) received a data request from the specified domain. For example, if the switch fails to update the database or is attacked (data injection), a message is generated to the primary FCS to try to correct and resynchronize with the rest of the switches in the fabric.

Recommended Action

Use the `secFabricShow` command to check whether any of the switches in the fabric encountered an error. If one or more of the switches is not in the ready state, and you have reason to believe that the error is the result of a possible security breach, take appropriate action as defined by your enterprise security policy.

SEC-1006**Message**

Security statistics error: Failed to reset due to invalid <data>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that invalid data has been received for any statistic-related command for security (`secStatsShow` or `secStatsReset`). The counter is updated automatically when a security violation occurs. This message may also occur if the updating counter fails.

Recommended Action

If the message is the result of a user command, retry the statistic command.

If the message persists, execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

SEC-1007**Message**

Security violation: Unauthorized host with IP address <IP address of the violating host> tries to establish API connection.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates a security violation was reported. The IP address of the unauthorized host is displayed in the message.

Recommended Action

Check for unauthorized access to the switch through the API connection.

SEC-1008**Message**

Security violation: Unauthorized host with IP address <IP address of the violating host> tries to establish HTTP connection.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates a security violation was reported. The IP address of the unauthorized host is displayed in the message.

Recommended Action

Check for unauthorized access to the switch through the HTTP connection.

SEC-1009**Message**

Security violation: Unauthorized host with IP address <IP address of the violating host> tries to establish TELNET connection.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates a security violation was reported. The IP address of the unauthorized host is displayed in the message.

Recommended Action

Check for unauthorized access to the switch through the Telnet connection.

SEC-1010**Message**

RCS rejected: <Reason String>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Trying to distribute the database from a non-primary switch.

Recommended Action

Resolve the specified error by executing the command only from the primary FCS.

SEC-1016

Message

Security violation: Unauthorized host with IP address <IP address of the violating host> tries to establish SSH connection.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates a security violation was reported. The IP address of the unauthorized host is displayed in the message.

Recommended Action

Check for unauthorized access to the switch through the SSH connection.

SEC-1022

Message

Failed to <operation> PKI objects.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates the fabric failed to generate or validate either the public or private key pair or the certificate signing request (CSR).

Recommended Action

Run the `secCertMgmt show -all` command and verify in FCAP row that all public key infrastructure (PKI) objects exist on the switch. If the private key does not exist, follow the steps for re-creating PKI objects. If a certificate does not exist or is invalid, install the certificate by following the field upgrade process.

SEC-1024

Message

The <DB name> security database is too large to fit in flash.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates the size of the security database is too large for the flash memory. The size of the security database increases with the number of entries in each policy.

Recommended Action

Reduce the size of the security database by reducing the number of entries within each policy.

SEC-1025**Message**

Invalid IP address (<IP address>) detected.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates a corruption occurred during the distribution of the security database. This can occur only when the primary fabric configuration server (FCS) distributes the security database to the other switches in the fabric, and then local validation finds the error in the security database. This is a rare occurrence.

Recommended Action

Run the `secFabricShow` command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database may not be correctly updated for that specific switch.

SEC-1026**Message**

Invalid format or character in switch member <switch member ID>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates a corruption occurred during the distribution of the security database. This can occur only when the primary fabric configuration server (FCS) distributes the security database to the other switches in the fabric, and then local validation finds the error in the security database. This is a rare occurrence.

Recommended Action

Run the `secFabricShow` command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database may not be correctly updated for that specific switch.

SEC-1028**Message**

No name is specified.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates a corruption occurred during the distribution of the security database. This can occur only when the primary fabric configuration server (FCS) distributes the security database to the other switches in the fabric, and then local validation finds the error in the security database. This is a rare occurrence.

Recommended Action

Run the `secFabricShow` command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database may not be correctly updated for that specific switch.

SEC-1029**Message**

Invalid character in <policy name>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates a corruption occurred during the distribution of the security database. This can occur only when the primary fabric configuration server (FCS) distributes the security database to the other switches in the fabric, and then local validation finds the error in the security database. This is a rare occurrence.

Recommended Action

Run the `secFabricShow` command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database may not be correctly updated for that specific switch.

SEC-1030**Message**

The length of the name is invalid.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates a corruption occurred during the distribution of the security database. This can occur only when the primary fabric configuration server (FCS) distributes the security database to the other switches in the fabric, and then local validation finds the error in the security database. This is a rare occurrence.

Recommended Action

Run the `secFabricShow` command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database may not be correctly updated for that specific switch.

SEC-1031**Message**

Current security policy DB cannot be supported by standby. CPs will go out of sync.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates the security database size is not supported by the standby control processor (CP).

Recommended Action

Reduce the security policy size by deleting entries within a policy or by deleting some policies.

SEC-1032**Message**

Empty FCS list is not allowed.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates a corruption occurred during the distribution of the security database. This can only occur when the primary fabric configuration server (FCS) distributes the security database to the other switches in the fabric, and then local validation finds the error in the security database. This is a rare occurrence.

Recommended Action

Run the `secFabricShow` command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database may not be correctly updated for that specific switch.

SEC-1033**Message**

Invalid character used in member parameter to add switch to SCC policy; command terminated.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates a member parameter in the `secPolicyAdd` command is invalid (for example, it may include an invalid character, such as an asterisk). A valid switch identifier (a WWN, a domain ID, or a switch name) must be provided as a member parameter in the `secPolicyAdd` command. Only the `secPolicyCreate` command supports use of the asterisk for adding switches to policies.

Recommended Action

Run the `secPolicyAdd` command using a valid switch identifier (WWN, domain ID, or switch name) to add specific switches to the Switch Connection Control (SCC) policy.

SEC-1034

Message

Invalid member <policy member>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates the input list has an invalid member.

Recommended Action

Verify the member names, and input the correct information.

SEC-1035

Message

Invalid device WWN <device WWN>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates the specified World Wide Name (WWN) is invalid.

Recommended Action

Enter the correct WWN value.

SEC-1036

Message

Device name <device name> is invalid due to a missing colon.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates one or more device names mentioned in the `secPolicyCreate` or `secPolicyAdd` commands does not have the colon character (:) as required.

Recommended Action

Run the `secPolicyCreate` or `secPolicyAdd` command with a properly formatted device name parameter.

SEC-1037**Message**

Invalid WWN format <invalid WWN>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates the WWN entered in the policy member list has an invalid format.

Recommended Action

Run the command again using the standard WWN format; 16 hexadecimal digits grouped as 8 colon-separated pairs, for example, 50:06:04:81:D6:F3:45:42.

SEC-1038**Message**

Invalid domain <domain ID>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates an invalid domain ID was entered.

Recommended Action

Verify that the domain ID is correct. If it is not, re-run the command using the correct domain ID.

SEC-1039**Message**

<message>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates the domain ID entered is out of range.

Recommended Action

Verify that the domain ID is correct. If it is not, re-run the command using the correct domain ID.

SEC-1040**Message**

Invalid portlist (<port list>). Cannot combine * with port member in the same portlist.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates the port list contains the wildcard asterisk (*) character. You cannot use the asterisk in a port list.

Recommended Action

Enter the port list values without any wildcard characters.

SEC-1041**Message**

Invalid port member <port member> in portlist (<port list>). <Reason>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates the port member is invalid for one of the following reasons:

- The value is not a number.
- The value is too long. Valid numbers must be between one and three characters long.
- The value cannot be parsed due to invalid characters.

Recommended Action

Use valid syntax when entering port members.

SEC-1042**Message**

Invalid index/area member <port member> in portlist (<Port list>). Out of range (<Minimum value> - <Maximum value>).

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates the specified index or area member is not within the minimum and maximum range.

Recommended Action

Use valid syntax when entering index or area numbers.

SEC-1043**Message**

Invalid port range <Minimum> - <Maximum>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates the specified port is not within the minimum and maximum range.

Recommended Action

Use valid syntax when entering port ranges.

SEC-1044**Message**

Duplicate member <member ID> in (<List>).

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates the specified member is a duplicate in the input list. The list can be a policy list or a switch member list.

Recommended Action

Do not specify any duplicates.

SEC-1045**Message**

Too many port members.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates a corruption occurred during the distribution of the security database. This can only occur when the primary fabric configuration server (FCS) distributes the security database to the other switches in the fabric, and then local validation finds the error in the security database. This is a rare occurrence.

Recommended Action

Run the `secFabricShow` command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database may not be correctly updated for that specific switch.

SEC-1046

Message

Empty list.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates a corruption occurred during the distribution of the security database. This can only occur when the primary fabric configuration server (FCS) distributes the security database to the other switches in the fabric, and then local validation finds the error in the security database. This is a rare occurrence.

Recommended Action

Run the `secFabricShow` command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database may not be correctly updated for that specific switch.

SEC-1049

Message

Invalid switch name <switch name>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates a corruption occurred during the distribution of the security database. This can only occur when the primary fabric configuration server (FCS) distributes the security database to the other switches in the fabric, and then local validation finds the error in the security database. This is a rare occurrence.

Recommended Action

Run the `secFabricShow` command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database may not be correctly updated for that specific switch.

SEC-1050

Message

There are more than one switches with the same name <switch name> in the fabric.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates a corruption occurred during the distribution of the security database. This can only occur when the primary fabric configuration server (FCS) distributes the security database to the other switches in the fabric, and then local validation finds the error in the security database. This is a rare occurrence.

Recommended Action

Run the `secFabricShow` command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database may not be correctly updated for that specific switch.

SEC-1051

Message

Missing brace for port list <port list>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates a corruption occurred during the distribution of the security database. This can only occur when the primary fabric configuration server (FCS) distributes the security database to the other switches in the fabric, and then local validation finds the error in the security database. This is a rare occurrence.

Recommended Action

Run the `secFabricShow` command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database may not be correctly updated for that specific switch.

SEC-1052

Message

Invalid input.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates a corruption occurred during the distribution of the security database. This can only occur when the primary fabric configuration server (FCS) distributes the security database to the other switches in the fabric, and then local validation finds the error in the security database. This is a rare occurrence.

Recommended Action

Run the `secFabricShow` command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database may not be correctly updated for that specific switch.

SEC-1053

Message

Invalid pFCS list <pFCS list>

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates a corruption occurred during the distribution of the security database. This can only occur when the primary fabric configuration server (FCS) distributes the security database to the other switches in the fabric, and then local validation finds these error in the security database. This is a rare occurrence.

Recommended Action

Run the `secFabricShow` command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database may not be correctly updated for that specific switch.

SEC-1054

Message

Invalid FCS list length <list length>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates a corruption occurred during the distribution of the security database. This can only occur when the primary fabric configuration server (FCS) distributes the security database to the other switches in the fabric, and then local validation finds the error in the security database. This is a rare occurrence.

Recommended Action

Run the `secFabricShow` command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database may not be correctly updated for that specific switch.

SEC-1055

Message

Invalid FCS list <WWN list>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates a corruption occurred during the distribution of the security database. This can only occur when the primary fabric configuration server (FCS) distributes the security database to the other switches in the fabric, and then local validation finds the error in the security database. This is a rare occurrence.

Recommended Action

Run the `secFabricShow` command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database may not be correctly updated for that specific switch.

SEC-1056

Message

Invalid position <New position>. Only <Number of members in FCS list> members in list.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates a corruption occurred during the distribution of the security database. This can only occur when the primary fabric configuration server (FCS) distributes the security database to the other switches in the fabric, and then local validation finds the error in the security database. This is a rare occurrence.

Recommended Action

Run the `secFabricShow` command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database may not be correctly updated for that specific switch.

SEC-1057

Message

No change. Both positions are the same.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates a corruption occurred during the distribution of the security database. This can only occur when the primary fabric configuration server (FCS) distributes the security database to the other switches in the fabric, and then local validation finds the error in the security database. This is a rare occurrence.

Recommended Action

Run the `secFabricShow` command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database may not be correctly updated for that specific switch.

SEC-1059

Message

Fail to <operation, e.g., save, delete, etc.,> <named item> to flash.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates the operation failed when writing to flash memory.

Recommended Action

Run the `supportFtp - e` command to FTP files from the switch and remove them from the flash memory.

SEC-1062

Message

Invalid number of Domains in Domain List.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that either no domains or domains more than the maximum number supported are specified.

Recommended Action

Enter the correct number of domains.

SEC-1063

Message

Failed to reset statistics.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that either the type or the domains specified are invalid.

Recommended Action

Enter valid input.

SEC-1064**Message**

Failed to sign message.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates the public key infrastructure (PKI) objects on the switch are not in a valid state and the signature operation failed.

Recommended Action

Run the `secCertMgmt show -all` command and verify in FCAP row that all PKI objects are valid. If PKI objects are not valid, generate the PKI objects and install the certificate by following the field upgrade process.

SEC-1065**Message**

Invalid character in list.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates the input list has an invalid character.

Recommended Action

Enter valid input.

SEC-1069**Message**

Security Database is corrupted.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates the security database is corrupted for unknown reasons.

Recommended Action

Execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

SEC-1071**Message**

No new security policy data to apply.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that no changes in the defined security policy database need to be activated at this time.

Recommended Action

Verify that the security event was planned. First change some policy definitions, and then run the `secPolicyActivate` command to activate the policies.

SEC-1072

Message

<Policy type> Policy List is Empty.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates the specific policy type is empty. The security database is corrupted for unknown reasons.

Recommended Action

Execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

SEC-1073

Message

No FCS policy in list.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates the specific policy type is empty. The security database is corrupted for unknown reasons.

Recommended Action

Execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

SEC-1074

Message

Cannot execute the command on this switch. Please check the secure mode and FCS status.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates a security command was run on a switch that is not allowed to run it either because it is in non-secure mode or because it does not have the required fabric configuration server (FCS) privilege.

Recommended Action

If a security operation that is not allowed in non-secure mode is attempted, do not perform the operation in non-secure mode. In secure mode, run the command from a switch that has the required privilege; that is, either a backup FCS or primary FCS.

SEC-1075**Message**

Fail to <operation> new policy set on all switches.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates a corruption occurred during the distribution of the security database. This can only occur when the primary fabric configuration server (FCS) distributes the security database to the other switches in the fabric, and then local validation finds the error in the security database. This is a rare occurrence.

Recommended Action

Run the `secFabricShow` command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database may not be correctly updated for that specific switch.

SEC-1076**Message**

NoNodeWWNZoning option has been changed.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates the NoNodeWWNZoning option has been changed. If the option is turned on, a zone member can be added using node WWNs, but the member will not be able to communicate with others nodes in the zone.

Recommended Action

Re-enable the current zone configuration for the change to take effect.

SEC-1077**Message**

Failed to activate new policy set on all switches.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates the policy could not be activated. Possible reasons that the policy could not be activated include not enough memory or a busy switch.

Recommended Action

Run the `secFabricShow` command to verify that all switches in the fabric are in the ready state. Retry the command when all switches are ready.

SEC-1078**Message**

No new data to abort.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates there are no new changes in the defined security policy database that can be aborted.

Recommended Action

Verify the security event was planned. Verify if there were really any changes to the defined policy database that can be aborted.

SEC-1079**Message**

The policy name <policy name> is invalid.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates the policy name entered in the `secPolicyCreate`, `secPolicyActivate`, `secPolicyAdd`, or `secPolicyDelete` command was invalid.

Recommended Action

Run the command again using a valid policy name.

SEC-1080**Message**

Operation denied. Please use `secPolicyActivate` or `distribute` commands.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates a corruption occurred during the distribution of the security database. This can only occur when the primary fabric configuration server (FCS) distributes the security database to the other switches in the fabric, and then local validation finds the error in the security database. This is a rare occurrence.

Recommended Action

Run the `fabricShow` command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database may not be correctly updated for that specific switch.

SEC-1081

Message

Entered a name for a DCC policy ID that was not unique.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates the Device Connection Control (DCC) policy name given in the `secPolicyCreate` command was the same as another DCC policy.

Recommended Action

Make sure that the DCC policy name has a unique alphanumeric string, and run the `secPolicyCreate` command again.

SEC-1082

Message

Failed to create <policy name> policy.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates the security policy was not created because of faulty input or low resources.

Recommended Action

Use proper syntax when creating policies. If the security database is too large, you must delete other members within the database before adding new members to a policy.

SEC-1083

Message

Name already exists.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates a corruption occurred during the distribution of the security database. This can only occur when the primary fabric configuration server (FCS) distributes the security database to the other switches in the fabric, and then local validation finds the error in the security database. This is a rare occurrence.

Recommended Action

Run the `fabricShow` command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database may not be correctly updated for that specific switch.

SEC-1084**Message**

Name exists for different type <Policy name>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates the specified policy already exists.

SEC-1085**Message**

Failed to create <policy name>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates the security policy was not created.

Recommended Action

Check that the current policy configuration is valid. For example, the RSNMP policy cannot exist without the WSNMP policy.

SEC-1086**Message**

The security database is too large to fit in flash.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates the security database has more data than the flash memory can accommodate.

Recommended Action

Reduce the number of entries in some policies to decrease the security database size.

SEC-1087**Message**

The security database is larger than the data distribution limit of fabric <fabric data distribution limit> bytes.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates the security database has more data than can be distributed to some of the switches in the fabric.

Recommended Action

Reduce the number of entries in the security policies to decrease the security database size.

SEC-1088**Message**

Cannot execute the command. Please try later.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates a corruption occurred during the distribution of the security database. This can only occur when the primary fabric configuration server (FCS) distributes the security database to the other switches in the fabric, and then local validation finds the error in the security database. This is a rare occurrence.

Recommended Action

Run the `fabricShow` command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database may not be correctly updated for that specific switch.

SEC-1089**Message**

Policy name <policy name> was not found.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates the security policy name in the `secPolicyAdd` command does not exist.

Recommended Action

Create the appropriate security policy first, and then use its name in the `secPolicyAdd` command to add new members.

SEC-1090**Message**

SCC list contains FCS member. Please remove member from the FCS policy first.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates a corruption occurred during the distribution of the security database. This can only occur when the primary fabric configuration server (FCS) distributes the security database to the other switches in the fabric, and then local validation finds the error in the security database. This is a rare occurrence.

Recommended Action

Run the `fabricShow` command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database may not be correctly updated for that specific switch.

SEC-1091**Message**

No policy to remove.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates the specified policy member does not exist or the policy itself does not exist.

Recommended Action

Verify that the security policy name or member ID is correct.

SEC-1092**Message**

<Policy name> Name not found.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates a corruption occurred during the distribution of the security database. This can only occur when the primary fabric configuration server (FCS) distributes the security database to the other switches in the fabric, and then local validation finds the error in the security database. This is a rare occurrence.

Recommended Action

Run the `fabricShow` command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database may not be correctly updated for that specific switch.

SEC-1093**Message**

New FCS list must have at least one member in common with current FCS list.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates the new fabric configuration server (FCS) list does not have a common member with the existing FCS list.

Recommended Action

Resubmit the command with at least one member of the new FCS list in common with the current FCS list.

SEC-1094**Message**

Policy member not found.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates a corruption occurred during the distribution of the security database. This can only occur when the primary fabric configuration server (FCS) distributes the security database to the other switches in the fabric, and then local validation finds that there is an error in the security database. This is a rare occurrence.

Recommended Action

Run the `fabricShow` command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database may not be correctly updated for that specific switch.

SEC-1095

Message

Deleting FCS policy is not allowed.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates a corruption occurred during the distribution of the security database. This can only occur when the primary fabric configuration server (FCS) distributes the security database to the other switches in the fabric, and then local validation finds the error in the security database. This is a rare occurrence.

Recommended Action

Run the `fabricShow` command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database may not be correctly updated for that specific switch.

SEC-1096

Message

Failed to delete <policy name> because <reason text>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates a policy cannot be removed because deleting it would result in an invalid security policy configuration.

Recommended Action

Verify the security policy configuration requirements and remove any policies that require the policy you want to be removed first.

SEC-1097

Message

Cannot find <active or defined> policy set.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates the specified policy could not be found.

Recommended Action

If the message persists, run `supportFtp` (as needed) to set up automatic FTP transfers; then run the `supportSave` command and contact your switch service provider.

SEC-1098**Message**

No <active or defined> FCS list.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates the specified policy could not be found.

Recommended Action

Execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

SEC-1099**Message**

Please enable your switch before running `secModeEnable`.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates a corruption occurred during the distribution of the security database. This can only occur when the primary fabric configuration server (FCS) distributes the security database to the other switches in the fabric, and then local validation finds the error in the security database. This is a rare occurrence.

Recommended Action

Run the `fabricShow` command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database may not be correctly updated for that specific switch.

SEC-1100**Message**

FCS switch present. Command terminated.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates a corruption occurred during the distribution of the security database. This can only occur when the primary fabric configuration server (FCS) distributes the security database to the other switches in the fabric, and then local validation finds the error in the security database. This is a rare occurrence.

Recommended Action

Run the `fabricShow` command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database may not be correctly updated for that specific switch.

SEC-1101**Message**

Failed to enable security on all switches. Please retry later.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates the security enable failed on the fabric because one or more switches in the fabric are busy.

Recommended Action

Verify that the security event was planned. If the security event was planned, run the `secFabricShow` command to verify that all switches in the fabric are in the ready state. When all switches are in the ready state, retry the operation.

SEC-1102**Message**

Fail to download <security data>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates the switch failed to download a certificate, security database, or policies. This can happen when the switch does not get enough resources to complete the operation, the fabric has not stabilized, or the policy database is an invalid format.

Recommended Action

Wait for the fabric to become stable and then retry the operation. If the policy database is in an illegal format (with `configDownload` command), correct the format and retry the operation.

SEC-1104**Message**

Fail to get primary <Certificate or public key>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates the switch failed to get either the primary certificate or a primary public key.

Recommended Action

Verify the primary switch has a valid certificate installed and retry the operation. If a valid certificate is not installed, install a certificate by following the procedure specified in the *Fabric OS Administrator's Guide*.

SEC-1105

Message

Fail to disable secure mode on all switches.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates the switch failed to disable security in the fabric. This could happen if the switch cannot get the required resources to complete the command, and sending to a remote domain fails or the remote domain returns an error.

Recommended Action

Run the `secFabricShow` to verify that all switches in the fabric are in the ready state. Retry the command when all switches are ready.

SEC-1106

Message

Failed to sign message data.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that some public key infrastructure (PKI) objects on the switch are not in a valid state, and a signature operation failed.

Recommended Action

Run the `secCertMgmt show -all` command and verify in FCAP row that all PKI objects exist on the switch. If a failure to validate PKI objects occurs, follow the steps for re-creating PKI objects.

SEC-1107

Message

Stamp is 0.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates a corruption occurred during the distribution of the security database. This can only occur when the primary fabric configuration server (FCS) distributes the security database to the other switches in the fabric, and then local validation finds the error in the security database. This is a rare occurrence.

Recommended Action

Run the `secFabricShow` command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database may not be correctly updated for that specific switch.

SEC-1108**Message**

Fail to reset stamp on all switches.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that a version reset operation failed either because the switch could not get all the required resources to perform the operation or because it failed to send the message to all switches in the fabric.

Recommended Action

Verify that the security event was planned. If the security event was planned, run the `secFabricShow` command to verify that all switches in the fabric are in the ready state. When all switches are in the ready state, retry the operation.

SEC-1110**Message**

FCS list must be the first entry in the [Defined Security policies] section. Fail to download defined database.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that a security policy download was attempted with a defined policy that does not have the fabric configuration server (FCS) policy as the first policy. The FCS policy is required to be the first policy in the defined security database.

Recommended Action

Download a correct configuration with the fabric configuration server (FCS) policy as the first policy in the defined security database.

SEC-1111

Message

New defined FCS list must have at least one member in common with current active FCS list. Fail to download defined database.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates the defined and active fabric configuration server (FCS) policy list failed to have at least one member in common.

Recommended Action

A new FCS policy list must have at least one member in common with the previous FCS policy.

SEC-1112

Message

FCS list must be the first entry in the Active Security policies, and the same as the current active FCS list in the switch.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates either a security policy download was attempted with an active policy that does not have the fabric configuration server (FCS) policy as the first policy, or the FCS policy is not the same as the current FCS policy on the switch.

Recommended Action

Make sure that the new FCS policy is the same as the current FCS policy on the switch.

SEC-1113**Message**

<Key> [<Feature> license] going to expire in <Expiry_days> day(s).

Message Type

LOG | AUDIT

Message Class

SECURITY

Message Severity

WARNING

Probable Cause

Indicates the license period will expire soon.

Recommended Action

Get a new license for this feature.

SEC-1114**Message**

<Key> [<Feature> license] has expired.

Message Type

LOG | AUDIT

Message Class

SECURITY

Message Severity

WARNING

Probable Cause

Indicates the license period has expired.

Recommended Action

Get a new license for this feature.

SEC-1115**Message**

No primary FCS to failover.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that during an attempted `secFcsFailover`, no primary FCS is present in the fabric.

Recommended Action

Run the `secFabricShow` command to verify that all switches in the fabric are in the ready state. When all switches are in the ready state, retry the operation.

SEC-1116**Message**

Fail to commit failover.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates a corruption occurred during the distribution of the security database. This can only occur when the primary fabric configuration server (FCS) distributes the security database to the other switches in the fabric, and then local validation finds the error in the security database. This is a rare occurrence.

Recommended Action

Run the `secFabricShow` command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database may not be correctly updated for that specific switch.

SEC-1117

Message

Fail to set <data>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates the switch failed to save the data received by the primary fabric configuration server (FCS) switch. This data can be an FCS password, a non-FCS password, SNMP data, or multiple user authentication data.

Recommended Action

Run the `fabricShow` command to verify that all switches in the fabric are in the ready state. When all switches are in the ready state, retry the operation.

SEC-1118

Message

Fail to set SNMP string.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates the SNMP string could not be set. Usually this problem is transient.

Recommended Action

Retry the command.

SEC-1119

Message

Secure mode has been enabled.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates the secure Fabric OS was enabled by the `secModeEnable` command.

Recommended Action

Verify the security event was planned. If the security event was planned, there is no action required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

SEC-1121

Message

Time is out of range when <text>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates the time on the switch is not synchronized with the primary fabric configuration server (FCS), the data packet is corrupted, or a replay attack is launched on the switch.

Recommended Action

Verify the security event was planned. If the security event was planned, verify that all switches in the fabric are in time synchronization with the primary FCS and that no external entity is trying to access the fabric. When verification is complete, retry the operation.

SEC-1122

Message

Error code: <Domain ID>, <Error message>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that one of the switches in the fabric could not communicate with the primary fabric configuration server (FCS).

Recommended Action

Run the `fabricShow` command to verify that all switches in the fabric are in the ready state. When all switches are in the ready state, retry the operation.

SEC-1123**Message**

Security database downloaded by Primary FCS.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates the security database was successfully downloaded from the primary fabric configuration server (FCS).

SEC-1124**Message**

Secure Mode is off.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that a secure mode disable is attempted in a non-secure fabric.

SEC-1126**Message**

Secure mode has been disabled.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that a secure mode disable operation completed successfully.

Recommended Action

Verify the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

SEC-1130**Message**

The Primary FCS has failed over to a new switch.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates a fabric configuration server (FCS) failover operation was completed successfully.

Recommended Action

Verify the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

SEC-1135**Message**

Secure fabric version stamp has been reset.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates the version stamp of the secure fabric is reset.

Recommended Action

Verify the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

SEC-1136**Message**

Failed to verify signature <data type, MUA, policy, etc.,>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates the receiving switch failed to validate the security database sent from the primary fabric configuration server (FCS) switch. This message usually indicates that the data package is corrupted, the time stamp on the package is out of range as a result of a replay attack or out-of-sync time service, or the signature verification failed. Signature verification failure indicates either an internal error (such as losing the primary public key) or an invalid database.

Recommended Action

Run the `secFabricShow` command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database may not be correctly updated for that switch. This message may also be the result of an internal corruption or a hacker attack to the secure fabric.

SEC-1137**Message**

No signature in <data type, MUA, policy, etc.,>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates the receiving switch failed to validate the security database sent from the primary fabric configuration server (FCS) switch. This message usually indicates that the data package is corrupted, the time stamp on the package is out of range as a result of a replay attack or out-of-sync time service, or the signature verification failed. Signature verification failure indicates either an internal error (such as losing the primary public key) or an invalid database.

Recommended Action

Run the `secFabricShow` command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database may not be correctly updated for that switch. This message may also be the result of an internal corruption or a hacker attack to the secure fabric.

SEC-1138**Message**

Security database download received from Primary FCS.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that a non-primary fabric configuration server (FCS) switch received a security database download.

Recommended Action

Verify that the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

SEC-1139**Message**

The RSNMP_POLICY cannot exist without the WSNMP_POLICY.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the receiving switch failed to validate the security database sent from the primary fabric configuration server (FCS) switch. This message usually indicates that the data package is corrupted, the time stamp on the package is out of range as a result of a replay attack or out-of-sync time service, or the signature verification failed. Signature verification failure indicates either an internal error (such as losing the primary public key) or an invalid database.

Recommended Action

Run the `secFabricShow` command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database may not be correctly updated for that switch. This message may also be the result of an internal corruption or a hacker attack to the secure fabric.

SEC-1142**Message**

Reject new policies. <reason text>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates the new policies are rejected because of the reason specified.

Recommended Action

Use proper syntax when entering policy information.

SEC-1145**Message**

A security admin event has occurred. This message is for information purpose only. The message for individual event is: <Event specific data>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates one of the following has occurred:

- The names for the specified policies have changed.
- The passwords have changed for the specified accounts.
- The SNMP community strings have been changed.

Recommended Action

Verify the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

SEC-1146

Message

PID changed: <State>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates the PID format of the switch was changed either to extended-edge PID or from extended-edge PID. If the Device Connection Control (DCC) policies existed, all index/area ID values either increased or decreased by 16. The values wrap around after 128. If a DCC policy contains an index/area of 127 before changing to extended-edge PID, then the new index/area is 15, because of the wraparound.

SEC-1153

Message

Error in RCA: RCS is not supported.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that reliable commit service (RCS) is not supported.

RCS must be capable on all switches in the fabric to be enabled. If all switches are capable, it is automatically enabled.

Recommended Action

For any switch that does not support RCS, obtain the latest firmware version from your switch supplier, and run the `firmwareDownload` command to upgrade the firmware.

If the message persists, execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

SEC-1154

Message

PID change failed: <Reason> <defined status> <active status>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that either the defined or the active policy could not be updated. If the policy database is very large, it might not be able to change the index/area because the new policy database exceeds the maximum size. This message can also be caused when the switch is short of memory. The status values can be either defined, active, or both. A negative value means that a policy set was failed by the daemon.

Recommended Action

Reduce the size of the policy database.

SEC-1155**Message**

PID change failed: <Reason> <defined status> <active status>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that either the defined or active policy was too large after modifying the index/area ID. The status values can be either defined, active, or both. A negative value means that a policy set was failed by the daemon.

Recommended Action

Reduce the size of the specified policy database.

SEC-1156**Message**

Change failed: <Reason> <defined status> <active status>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates the security daemon is busy. The status values can be defined, active, or both. A negative value means that a policy set was failed by the daemon.

Recommended Action

For the first reject, wait a few minutes and then resubmit the transaction. Fabric-wide commands may take a few minutes to propagate throughout the fabric. Make sure to wait a few minutes between executing commands so that your commands do not overlap in the fabric.

SEC-1157**Message**

PID Change failed: <Reason> <defined status> <active status>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates the provisioning resources for a security policy failed because of low memory or internal error. The status values can be defined, active, or both. A negative value means that a policy set was failed by the daemon.

Recommended Action

Retry the failed command.

If the message persists, execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

SEC-1158**Message**

Invalid name <Policy or Switch name>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates the specified name is invalid. The name can be a policy name or a switch name.

Recommended Action

Enter a valid name.

SEC-1159**Message**

Non_Reachable domain <Domain ID>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates a corruption occurred during the distribution of the security database. This can only occur when the primary fabric configuration server (FCS) distributes the security database to the other switches in the fabric, and then local validation finds the error in the security database. This is a rare occurrence.

Recommended Action

Run the `secFabricShow` command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database may not be correctly updated for that specific switch.

SEC-1160**Message**

Duplicate port <port ID> in port list (<port list>).

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates a duplicate port member exists in the specified port list.

Recommended Action

Verify that there is no duplicate port member in the port list.

SEC-1163

Message

System is already in secure mode. Lockdown option cannot be applied.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates the lockdown option was attempted while the fabric is in secure mode.

Recommended Action

Do not use the lockdown option with the `secModeEnable` command when a switch is already in secure mode.

SEC-1164

Message

Lockdown option cannot be applied on a non-FCS switch.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates the attempt to enable security is made on a switch that is not present in the fabric configuration server (FCS) list.

Recommended Action

Add the switch to the FCS policy list when using the lockdown option to enable security.

SEC-1165

Message

Low memory, failed to enable security on all switches.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates the system is low on memory.

Recommended Action

Wait a few minutes and try the command again.

SEC-1166

Message

Non FCS tries to commit failover.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates a corruption occurred during the distribution of the security database. This can only occur when the primary fabric configuration server (FCS) distributes the security database to the other switches in the fabric, and then local validation finds the error in the security database. This is a rare occurrence.

Recommended Action

Run the `secFabricShow` command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database may not be correctly updated for that specific switch.

SEC-1167

Message

Another FCS failover is in process. Command terminated.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that because another failover is already in progress, this failover attempt cannot proceed.

Recommended Action

Verify the security event was planned. If the security event was planned, retry fabric configuration server (FCS) failover after the current failover has completed, if this switch should become the primary FCS. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

SEC-1168**Message**

Primary FCS failover is busy. Please retry later.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates a corruption occurred during the distribution of the security database. This can only occur when the primary fabric configuration server (FCS) distributes the security database to the other switches in the fabric, and then local validation finds the error in the security database. This is a rare occurrence.

Recommended Action

Run the `secFabricShow` command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database may not be correctly updated for that specific switch.

SEC-1170**Message**

This command must be executed on the Primary FCS switch, the first reachable switch in the FCS list.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates a corruption occurred during the distribution of the security database. This can only occur when the primary fabric configuration server (FCS) distributes the security database to the other switches in the fabric, and then local validation finds the error in the security database. This is a rare occurrence.

Recommended Action

Run the `secFabricShow` command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database may not be correctly updated for that specific switch.

SEC-1171**Message**

Disabled secure mode due to invalid security object.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates the switch is segmented, and secure mode is disabled on the switch because there was no license present or no public key infrastructure (PKI) objects.

Recommended Action

Run the `secCertMgmt show -all` command and verify in FCAP row whether all PKI objects exist. If they do not exist, run the `secCertMgmt` command to create them for the switch.

Run the `licenseAdd` command to install the required license key. Contact your switch supplier to obtain a license if you do not have one.

SEC-1172**Message**

Failed to identify role.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates the switch is unable to determine its role (primary FCS or backup FCS) in the secure fabric.

Recommended Action

Verify all switches in the fabric are in time synchronization with the primary FCS and that no external entity is trying to access the fabric. When verification is complete, retry the operation.

SEC-1173

Message

Lost contact with Primary FCS switch.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates the switch has lost contact with the primary fabric configuration server (FCS) switch in the secure fabric. This could result from the primary FCS being disabled.

Recommended Action

If the primary FCS was disabled intentionally, no action is required; if not, check the primary FCS.

SEC-1174

Message

Failed to set <FCS or non-FCS> password.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates the fabric configuration server (FCS) or non-FCS password could not be set.

Recommended Action

Verify all switches in the fabric are in time synchronization with the primary FCS and that no external entity is trying to access the fabric. When verification is complete, retry the operation.

SEC-1175

Message

Failed to install zone data.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates the zone database could not be installed on the switch.

Recommended Action

Verify all switches in the fabric are in time synchronization with the primary FCS and that no external entity is trying to access the fabric. When verification is complete, retry the operation.

SEC-1176**Message**

Failed to generate new version stamp.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates the primary fabric configuration server (FCS) failed to generate a new version stamp because the fabric was not stable.

Recommended Action

Verify all switches in the fabric are in time synchronization with the primary FCS and that no external entity is trying to access the fabric. When verification is complete, retry the operation.

SEC-1180**Message**

Added account <user name> with <role name> authorization.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates the specified new account has been created.

SEC-1181**Message**

Deleted account <user name>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates the specified account has been deleted.

SEC-1182**Message**

Recovered <number of> accounts.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates the specified number of accounts has been recovered from backup.

SEC-1183**Message**

Policy to binary conversion error: Port <port number> is out range.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates a security database conversion has failed because of an invalid value.

Recommended Action

Retry the command with a valid value.

If the message persists, execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

SEC-1184**Message**

<Security server (RADIUS/LDAP/TACACS+)> configuration change, action <action>, server ID <server name>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates the specified action is applied to the specified remote authentication dial-in user service (RADIUS/LDAP/TACACS+) server configuration. The possible actions are ADD, REMOVE, CHANGE, and MOVE.

SEC-1185**Message**

<action> switch DB.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates the switch database was enabled or disabled as the secondary authentication, authorization, and accounting (AAA) mechanism when remote authentication dial-in user service (RADIUS/LDAP/TACACS+) is the primary AAA mechanism.

SEC-1186

Message

<Security server (RADIUS/LDAP/TACACS+)> <action> Configuration.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates the RADIUS, LDAP, or TACACS+ configuration was enabled or disabled as the primary authentication, authorization, and accounting (AAA) mechanism.

SEC-1187

Message

Security violation: Unauthorized switch <switch WWN> tries to join fabric.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates a Switch Connection Control (SCC) security violation was reported. The specified unauthorized switch attempts to join the fabric.

Recommended Action

Check the SCC policy to verify the switches allowed in the fabric. If the switch should be allowed in the fabric but it is not included in the SCC policy, add the switch to the policy. If the switch is not allowed access to the fabric, this is a valid violation message and an unauthorized entity is trying to access your fabric. Take appropriate action, as defined by your enterprise security policy.

SEC-1188

Message

Security violation: Unauthorized device <device node name> tries to FLOGI to index/area <port number> of switch <switch WWN>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates a Device Connection Control (DCC) security violation was reported. The specified device attempted to log in using fabric login (FLOGI) to an unauthorized port. The DCC policy correlates specific devices to specific port locations. If the device changes the connected port, the device will not be allowed to log in.

Recommended Action

Check the DCC policy and verify the specified device is allowed in the fabric and is included in the DCC policy. If the specified device is not included in the policy, add it to the policy. If the host is not allowed access to the fabric, this is a valid violation message and an unauthorized entity is trying to access your fabric. Take appropriate action, as defined by your enterprise security policy.

SEC-1189**Message**

Security violation: Unauthorized host with IP address <IP address> tries to do SNMP write operation.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates an SNMP security violation was reported. The specified unauthorized host attempted to perform a write SNMP operation.

Recommended Action

Check the WSNMP policy and verify which hosts are allowed access to the fabric through SNMP. If the host is allowed access to the fabric but is not included in the policy, add the host to the policy. If the host is not allowed access to the fabric, this is a valid violation message and an unauthorized entity is trying to access your fabric. Take appropriate action, as defined by your enterprise security policy.

SEC-1190**Message**

Security violation: Unauthorized host with IP address <IP address> tries to do SNMP read operation.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates an SNMP security violation was reported. The specified unauthorized host attempted to perform a read SNMP (RSNMP) operation.

Recommended Action

Check the RSNMP policy to verify the hosts allowed access to the fabric through SNMP read operations are included in the RSNMP policy. If the host is allowed access but is not included in the RSNMP policy, add the host to the policy. If the host is not allowed access to the fabric, this is a valid violation message and an unauthorized entity is trying to access your fabric. Take appropriate action, as defined by your enterprise security policy.

SEC-1191**Message**

Security violation: Unauthorized host with IP address <Ip address> tries to establish HTTP connection.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates an HTTP security violation was reported. The specified unauthorized host attempted to establish an HTTP connection.

Recommended Action

Determine whether the host IP address specified in the message can be used to manage the fabric through an HTTP connection. If so, add the host IP address to the HTTP policy of the fabric. If the host is not allowed access to the fabric, this is a valid violation message and an unauthorized entity is trying to access your fabric. Take appropriate action, as defined by your enterprise security policy.

SEC-1192**Message**

Security violation: Login failure attempt via <connection method>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates a serial or modem login security violation was reported. The wrong password was used while trying to log in through a serial or modem connection; the login failed.

Recommended Action

Use the correct password.

SEC-1193**Message**

Security violation: Login failure attempt via <connection method>. IP Addr: <IP address>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates a specified login security violation was reported. The wrong password was used while trying to log in through the specified connection method; the login failed.

Recommended Action

The error message lists the violating IP address. Verify that this IP address is being used by a valid switch admin. Use the correct password.

SEC-1194**Message**

This switch does not have all the required PKI objects correctly installed.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates a corruption occurred during the distribution of the security database. This can only occur when the primary fabric configuration server (FCS) distributes the security database to the other switches in the fabric, and then local validation finds the error in the security database. This is a rare occurrence.

Recommended Action

Run the `secFabricShow` command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database may not be correctly updated for that specific switch.

SEC-1195**Message**

This switch has no <component> license.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates a corruption occurred during the distribution of the security database. This can only occur when the primary fabric configuration server (FCS) distributes the security database to the other switches in the fabric, and then local validation finds the error in the security database. This is a rare occurrence.

Recommended Action

Run the `secFabricShow` command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database may not be correctly updated for that specific switch.

SEC-1196**Message**

Switch does not have all default account names.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates the default switch accounts admin and user do not exist on the switch when enabling security.

Recommended Action

Reset the default admin and user account names on the switch that reported the warning and retry enabling security.

SEC-1197**Message**

Changed account <user name>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates the specified account has changed or password is changed from WebEM.

SEC-1198**Message**

Security violation: Unauthorized host with IP address <IP address> tries to establish API connection.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates an API security violation was reported. The specified unauthorized host attempted to establish an API connection.

Recommended Action

Check to see if the host IP address specified in the message can be used to manage the fabric through an API connection. If so, add the host IP address to the API policy of the fabric. If the host is not allowed access to the fabric, this is a valid violation message and an unauthorized entity is trying to access your fabric. Take appropriate action, as defined by your enterprise security policy.

SEC-1199**Message**

Security violation: Unauthorized access to serial port of switch <switch instance>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates a serial connection policy security violation was reported. An attempt was made to access the serial console on the specified switch instance when it is disabled.

Recommended Action

Check to see if an authorized access attempt is being made on the console. If so, add the switch WWN to the serial policy. If the host is not allowed access to the fabric, this is a valid violation message and an unauthorized entity is trying to access your fabric. Take appropriate action, as defined by your enterprise security policy.

SEC-1200**Message**

Security violation: MS command is forwarded from non-primary FCS switch.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates a management server (MS) forward security violation was reported. A management server command was forwarded from a non-primary fabric configuration server (FCS) switch.

Recommended Action

Check the MS policy and verify that the connection is allowed. If the connection is allowed but not specified, enable the connection in the MS policy. If the MS policy does not allow the connection, this is a valid violation message and an unauthorized entity is trying to access your fabric. Take appropriate action, as defined by your enterprise security policy.

SEC-1201**Message**

Security violation: MS device <device WWN> operates on non-primary FCS switch.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates a management server (MS) operation security violation was reported. An MS device operation occurred on a non-primary fabric configuration server (FCS) switch.

Recommended Action

Check the management server policy and verify the connection is allowed. If the connection is allowed but not specified, enable the connection in the MS policy. If the MS policy does not allow the connection, this is a valid violation message and an unauthorized entity is trying to access your fabric. Take appropriate action, as defined by your enterprise security policy.

SEC-1202**Message**

Security violation: Unauthorized access from MS device node name <device node name>, device port name <device port name>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates a management server (MS) security violation was reported. The unauthorized device specified in the message attempted to establish a connection.

Recommended Action

Check the MS server policy and verify that the connection is allowed. If the connection is allowed but not specified, enable the connection in the MS policy. If the MS policy does not allow the connection, this is a valid violation message and an unauthorized entity is trying to access your fabric. Take appropriate action, as defined by your enterprise security policy.

SEC-1203**Message**

Login information: Login successful via: <Login method>. IP Addr: <IP address>

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates the IP address of the remote station logging in.

SEC-1250**Message**

DCC enforcement API failed: <failed action> err=<status>, key=<data>

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates an internal error caused the Device Connection Control (DCC) policy enforcement to fail.

Recommended Action

Retry the failed security command.

If the message persists, run `supportFtp` (as needed) to set up automatic FTP transfers; then run the `supportSave` command and contact your switch service provider.

SEC-1251**Message**

Policy to binary conversion error: <text message> <value>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates the security database conversion failed because of invalid values. The reason is specified in the *text message* variable and the faulty value is printed in the *value* variable.

Recommended Action

Retry the failed security command.

If the message persists, run `supportFtp` (as needed) to set up automatic FTP transfers; then run the `supportSave` command and contact your switch service provider.

SEC-1253

Message

Bad DCC interface state during <Phase>, state=<state>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates an internal error has caused the Device Connection Control (DCC) policy update to fail in the provision, commit, or cancel phases.

Recommended Action

Retry the failed security command.

If the message persists, run `supportFtp` (as needed) to set up automatic FTP transfers; then run the `supportSave` command and contact your switch service provider.

SEC-1300

Message

This switch is in VcEncode mode. Security is not supported.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates the switch is set up with VC-encoded mode.

Recommended Action

Turn off VC-encoded mode before enabling security.

SEC-1301

Message

This switch is in interop mode. Security is not supported.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates the switch is enabled in interop mode.

Recommended Action

Disable interop mode using the `interopMode` command before enabling the Secure Fabric OS feature.

SEC-1302

Message

This switch does not have all the required PKI objects correctly installed.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates a corruption occurred during the distribution of the security database. This can only occur when the primary fabric configuration server (FCS) distributes the security database to the other switches in the fabric, and then local validation finds the error in the security database. This is a rare occurrence.

Recommended Action

Run the `secFabricShow` command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database may not be correctly updated for that specific switch.

SEC-1303

Message

This software version does not support security.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates the currently installed software version does not support the Brocade Secure Fabric OS feature.

Recommended Action

Run the `firmwareDownload` command to update the firmware to the latest version for your specific switch. Verify the firmware you are installing supports the Brocade Secure Fabric OS feature.

SEC-1304**Message**

This switch has no security license.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates a corruption occurred during the distribution of the security database. This can only occur when the primary fabric configuration server (FCS) distributes the security database to the other switches in the fabric, and then local validation finds the error in the security database. This is a rare occurrence.

Recommended Action

Run the `secFabricShow` command to verify the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database may not be correctly updated for that specific switch.

SEC-1305**Message**

This switch has no zoning license.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates a corruption occurred during the distribution of the security database. This can only occur when the primary fabric configuration server (FCS) distributes the security database to the other switches in the fabric, and the local validation finds the error in the security database. This is a rare occurrence.

Recommended Action

Run the `secFabricShow` command to verify the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database may not be correctly updated for that specific switch.

SEC-1306**Message**

Failed to verify certificate with root CA.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates the certificate could not be verified with root certificate authority (CA). This could happen if an unauthorized switch tries to access the fabric that is not certified by a trusted root CA or a root CA certificate does not exist on the switch.

Recommended Action

Run the `secCertMgmt show -all` command and verify in FCAP row that all public key infrastructure (PKI) objects exist on the switch. If a failure to validate PKI objects occurs, follow the steps for re-creating PKI objects. If PKI objects are valid, verify that an unauthorized switch is not trying to access the fabric.

SEC-1307**Message**

<Security server (RADIUS/LDAP/TACACS+)> server <Server name> authenticated user account '<username>'.
<RADIUS/LDAP/TACACS+ local authorization>

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that after some servers timed out, the specified RADIUS, LDAP, or TACACS+ server responded to a switch request when a RADIUS/LDAP/TACACS+ user is authorized using switch local database.

Recommended Action

If the message appears frequently, move the responding server to the top of the RADIUS/LDAP/TACACS+ server configuration list using the `aaaConfig` command or configure remote authorization for LDAP user.

SEC-1308**Message**

All <RADIUS/LDAP/TACACS+ server identity> servers failed to authenticate user account '<username>'.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that all servers in the RADIUS, LDAP, or TACACS+ configuration have failed to respond to a switch request within the specified timeout. For RADIUS PEAP-MSCHAPv2 authentication with a Windows server, if the user account name matches that of a role/group on the server with administrative privileges such as "admin" or "maintenance", this message will be displayed as well.

Recommended Action

Verify that the switch has proper network connectivity to the specified RADIUS, LDAP, or TACACS servers and that the servers are correctly configured.

SEC-1309**Message**

Waiting for RCS transaction to complete: <Wait time in seconds> secs

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that Fabric OS is still waiting for the reliable commit service (RCS) transaction to complete.

Recommended Action

Verify if there are any reliable commit service (RCS) or Reliable Transport With Response (RTWR) errors. If not, the transaction is still in progress.

SEC-1310**Message**

Unable to determine data distribution limit of fabric. Please retry later.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates the data distribution limit could not be obtained from all switches in the fabric. This may happen if the fabric is reconfiguring or a new domain joined the fabric.

Recommended Action

Retry the command when the fabric is stable.

SEC-1311**Message**

Security mode cannot be enabled because one or more of the password policies is not set to default value.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates the security enable failed on the fabric because one or more switches in the fabric have password policies that are not set to the default values.

Recommended Action

Verify the security event was planned.

If the security event was planned, run the `passwdCfg --setdefault` command on each switch in the fabric to set the password policies to the default values. Then verify with the `passwdCfg --showall` command that password policies are set to the default values on all switches and retry the `secModeEnable` command.

SEC-1312

Message

<MESG Message>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates the password configuration parameters changed.

Recommended Action

Verify the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

SEC-1313

Message

The passwdcfg parameters were set to default values.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates the password configuration parameters were set to default values.

Recommended Action

Verify the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

SEC-1314

Message

Reading <IP Address Description> IP address from EM failed.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates the call to the environment monitor (EM) module to retrieve the IP address failed.

Recommended Action

Reboot the system to fix this error. If the problem persists, contact your switch service provider.

SEC-1315**Message**

<Name of command> command failed -<List of databases rejecting distribution> db(s) configured for rejection on this switch.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates there was an attempt to distribute databases to a switch that was configured not to accept distributions from the fabric.

Recommended Action

Verify the accept distribution configuration for the listed databases. Use the `remoteeCfg` command to verify and correct the configuration if necessary.

SEC-1316**Message**

<Policy Name> policy WWN List is conflicting with domain <Domain Number>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates the newly added switches to the fabric, as specified by domain number, have a conflicting policy with the local switch.

Recommended Action

Check the conflicting policy and make the new switches and the local switch policies the same.

SEC-1317**Message**

Inconsistent fabric, rejecting transaction

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that either this domain is performing FDD merge or matched domains are not the same as what CM sees.

Recommended Action

If a policy conflict exists, resolve it, and then wait for the fabric to become stable. Retry the distribution.

SEC-1318**Message**

Transaction rejected due to inconsistent fabric.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that some domains detected an inconsistent fabric.

Recommended Action

Resolve the policy conflict, if there is one, and then wait for the fabric to stabilize. Retry the distribution.

SEC-1319

Message

<Event name> updated<Datasets updated> dbs(s).

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates the specified event has occurred.

Recommended Action

Verify the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

SEC-1320

Message

Non-acl domain <Domain Number> tries to join a fabric with strict fabric wide policy.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that a domain not supporting an access control list (ACL) policy tried to join a fabric with the strict fabric-wide policy.

Recommended Action

No action is required. The domain is denied by disallowing all its E_Ports from connecting to the fabric.

SEC-1321

Message

Failed secure mode enable command. Reason: <Reason>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates the security enable failed on the fabric because the switch has a conflicting configuration such as fabric-wide consistency configuration or AD configuration.

Recommended Action

Verify the security event was planned. If the security event was planned, run the `fddCfg --fabwideset` command or `ad --clear` command to clear the fabric wide consistency configuration or AD configuration and retry the `secModeEnable` command.

SEC-1322**Message**

Some DCC policy is too large, distribution cancelled.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates this fabric is not able to support a Device Connection Control (DCC) policy with more than 256 ports.

Recommended Action

Reconfigure any policy that includes more than 256 ports in its member list, and then save the policy configuration changes.

SEC-1323**Message**

Key(s) \"<Key Name>\" ignored during configdownload.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates the specified key is ignored during configuration download.

Recommended Action

Verify the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

SEC-1324**Message**

Fabric transaction failure. RCS error: <Error code>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates the reliable commit service (RCS) transaction failed with the specified reason code.

Recommended Action

Verify the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

SEC-1325**Message**

Security enforcement: Switch <switch WWN> connecting to port <Port number> is not authorized to stay in fabric.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that because of a Switch Connection Control (SCC) policy violation, the switch is being disabled on the specified port.

Recommended Action

No action is required unless the switch must remain in the fabric. If the switch must remain in the fabric, add the switch World Wide Name (WWN) to the SCC policy, and then attempt to join the switch with the fabric.

SEC-1326

Message

Event: fddcfg --fabwideset, Status: success, Info: Fabric wide configuration set to <Fabric-wide configuration set by user>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates the specified event has occurred.

Recommended Action

Verify the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

SEC-1327

Message

Strict <Policy Name> policy WWN List is conflicting with domain <Domain Number>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates the policy is conflicting with the domain.

Recommended Action

No action is required. The domain is denied by disallowing all its E_Ports connected to the fabric. If the domain should be allowed to merge with the fabric, then resolve the issue by making the conflicting policies the same.

SEC-1328

Message

Attempt to enable secure mode failed. Reason: <Reason>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates the `secModeEnable` command failed on the fabric because the Authentication Policy is enabled on the switch.

Recommended Action

Verify the security event was planned. If the security event was planned, run the `authUtil --policy passive` command to disable the Authentication Policy and retry the `secModeEnable` command.

SEC-1329**Message**

IPFilter enforcement:Failed to enforce ipfilter policy of <Policy Type> type because of <Error code>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates the IP filter policy enforcement failed because of an internal system failure.

Recommended Action

Execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

SEC-1330**Message**

<Name of command> command failed -<List of databases rejecting distribution> db(s) are coming from a non-Primary switch.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates an attempt was made to distribute databases either from a backup fabric configuration server (FCS) switch or a non-FCS switch.

Recommended Action

Verify the distribution is initiated by the FCS switch. Use the `secPolicyShow` command to verify and correct the configuration if necessary.

SEC-1331**Message**

Attempt to enable secure mode failed. Reason: <Reason>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates the `secModeEnable` command failed on the fabric because default IP filter policies are not active on the switch, or an active transaction exists on IP filter policies.

Recommended Action

Verify the security event was planned.

If the security event was planned, run the `ipfilter --activate default_ipv4` command or the `ipfilter --activate default_ipv6` command to activate default IP filter policies. Use the `ipfilter --save` or `ipfilter --transabort` commands to save or abort the active transaction on IP filter policies. Then retry the `secModeEnable` command.

SEC-1332**Message**

Fabric wide policy is conflicting as <Policy Name> is present in the fabric wide policy and 5.3 or 5.2 switches present in the fabric.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates the fabric-wide policy is conflicting.

Recommended Action

Remove either the FCS from the fabric-wide policy, or remove Fabric OS v5.3 or Fabric OS v5.2 switches from the fabric, or set the fabric-wide mode for FCS as strict.

SEC-1333**Message**

<Name of command> command failed. There are <List of databases rejecting distribution> in fabric. <printf> db(s) distribution is blocked.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates there was an attempt to distribute PWD/IPFILTER databases from the fabric to a VF-enabled switch or distribute PWD from a fabric to a switch having user(s) with user-defined role(s).

Recommended Action

Disable VF on all the switches that have VF-enabled or delete all users with user-defined role(s) if PWD or IPFILTER databases need to be distributed.

SEC-1334**Message**

SSH Daemon is restarted.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates the Secure Shell (SSH) daemon was not running and it was restarted.

SEC-1335**Message**

Strict <Policy Name> policy is conflicting with domain <Domain Number>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates the policy is conflicting with the domain.

Recommended Action

No action is required. The domain is denied by disallowing all its E_Ports connected to the fabric. If the domain should be allowed to merge with the fabric, then resolve the issue by making the conflicting policies the same.

SEC-1336**Message**

<Policy Name> policy is conflicting with domain <Domain Number>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates the newly added switches to the fabric, as specified by domain number, have a conflicting policy with the local switch.

Recommended Action

Check the conflicting policy and make the new switches and the local switch policies the same.

SEC-1337**Message**

Plain-text password is sent during console login

Message Type

AUDIT | LOG

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates that plain-text password is sent during console login

Recommended Action

Verify the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

SEC-1338**Message**

<MESG Message>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates the password configuration parameters changed.

Recommended Action

Verify the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

SEC-1339**Message**

Distribute command failed. There are Inflight encryption enabled switch(s) in fabric. Auth db(s) distribution is blocked

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates there was an attempt to distribute AUTH databases with switch policy (Off/Passive) from the fabric to a switch that has Inflight Encryption enabled

Recommended Action

Disable or enable Inflight encryption in all the switches in the fabric

SEC-1340**Message**

<Message>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the Device Connection Control (DCC) policy member is configured incorrectly.

Recommended Action

Verify that the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

SEC-1341**Message**

Failed to update client capability to ESS (Exchange Switch Support) after maximum number of retries - return code <Failed return code>. Failing sync dump to standby CP.

Message Type

AUDIT | LOG

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates that Exchange Switch Support (ESS) is unable to update its capability. Failed to send the sync dump to standby control processor (CP).

Recommended Action

Verify that HA synchronization has failed using the `haShow` command. If HA synchronization has failed, execute the `haSyncStart` command on active CP to resynchronize the HA state.

SEC-1342

Message

HIF mode is enabled. <Warning>

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the local switch received a remote distribution for Switch Connection Control (SCC) policy or fabric-wide data distribution configuration. This may modify SCC policy or strict SCC mode configuration in Fabric Data Distribution (FDD). This configuration change may lead to unexpected behavior when High Integrity Fabrics (HIF) is enabled.

Recommended Action

Verify that the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

SEC-1343

Message

PWD policy distributed successfully from Switch <Switch WWN>. User configuration and Password configuration is enforced successfully.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates password database distribute from switch is successful in the Access Gateway (AG) mode.

Recommended Action

Verify the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

SEC-1344

Message

Frequency of security violations exceed limit. Counters will be dropped

Message Type

AUDIT | LOG

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates that violation counter updates may be dropped. High number of security violations on the switch.

Recommended Action

Identify and address the reason for security violations.

SEC-1345**Message**

Analytics platform has taken over as FCS primary.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the analytics platform switch has taken over as primary Fabric Configuration Server (FCS) for the fabric connected. This is not a valid configuration.

Recommended Action

After switchdisable in Analytics Monitoring Platform (AMP), delete the FCS_POLICY and activate the policy using the `secPolicyActivate` command. Correct the order of FCS policy in the fabric and activate it. Enable the AMP switch and distribute the corrected FCS_POLICY from the connected fabric.

SEC-1346**Message**

Possible Denial of Service attack detected on Management Ports.

Message Type

AUDIT | LOG

Message Class

SECURITY

Message Severity

WARNING

Probable Cause

Indicates that a Denial of Service attack is detected on Management ports.

SEC-1347**Message**

<Security server (RADIUS/LDAP/TACACS+)> server <Server name> reachable, but failed to validate or authorize the user account '<username>'.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that AAA server is reachable but failed to authenticate due to invalid user or invalid credentials or invalid authorization.

Recommended Action

Verify the user/password entered for the specified RADIUS, LDAP, or TACACS+s server is correct.

SEC-1348**Message**

Maximum limit for policy members reached.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the limit for the number of members for that security policy has been reached.

Recommended Action

Delete the members that would never be part of the fabric so that new members can be added.

SEC-1349**Message**

Security violation: Service shell token authentication failed.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates a failed attempt to authenticate to service shell due to invalid authentication token.

Recommended Action

Verify the authentication token used is correct.

SEC-1350**Message**

Config save operation failed with error <error code>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the config save operation to sync the file across partition and CPs got failed.

Recommended Action

Verify HA state is in sync between the CPs and retry the operation.

SEC-1351**Message**

Security violation: Factory shell token authentication failed.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates a failed attempt to authenticate to factory shell due to invalid authentication token.

Recommended Action

Verify the authentication token used is valid.

SEC-1352**Message**

Authentication failed for RSA user '<username>' with response '<RSA SecurID server response code>'.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates authentication failure for RSA SecurID user with server response code.

Recommended Action

Verify the authentication credentials are valid. Check the server response code and resolve the error on the RSA SecurID server.

SEC-3001**Message**

Event: <Event Name>, Status: success, Info: Security mode <State change: Enabled or Disabled> on the fabric.

Message Type

AUDIT

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates the security mode of the fabric was either enabled or disabled.

Recommended Action

Verify the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

SEC-3002**Message**

Event: <Event Name>, Status: success, Info: <Event Related Info>.

Message Type

AUDIT

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates the specified security event has occurred. The event can be one of the following:

- There has been a fabric configuration server (FCS) failover.
- A security policy has been activated.
- A security policy has been saved.
- A security policy has been aborted.
- A non-FCS password has changed.

Recommended Action

Verify the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

SEC-3003**Message**

Event: <Event Name>, Status: success, Info: Created <Policy Name> policy, with member(s) <Member List> .

Message Type

AUDIT

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates a new security policy with entries has been created. When you use a wildcard (for example, an asterisk) in creating a policy, the audit report displays the wildcard in the event information field.

Recommended Action

Verify the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

SEC-3004**Message**

Event: <Event Name>, Status: success, Info: Created <Policy name> policy.

Message Type

AUDIT

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates a new security policy has been created. When you use a wildcard (for example, an asterisk) in creating a member for a policy, the audit report displays the wildcard in the event information field.

Recommended Action

Verify the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

SEC-3005**Message**

Event: <Event Name>, Status: success, Info: Added member(s) <Members added> to policy <Policy name>.

Message Type

AUDIT

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates new members have been added to a security policy. If you use a wildcard (for example, an asterisk) in adding members to a policy, the audit report displays the wildcard in the event information field.

Recommended Action

Verify the addition of members to the policy was planned. If the addition of members was planned, no action is required. If the addition of members was not planned, take appropriate action as defined by your enterprise security policy.

SEC-3006**Message**

Event: <Event Name>, Status: success, Info: Removed member(s) <Members removed> from policy <Policy name>.

Message Type

AUDIT

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates a user has removed the specific members from the security policy. When you use a wildcard (for example, an asterisk) in removing members from a policy, the audit report displays the wildcard in the event information field.

Recommended Action

Verify the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

SEC-3007**Message**

Event: <Event Name>, Status: success, Info: Deleted policy <Deleted policy name>.

Message Type

AUDIT

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates the specified security policy was deleted.

Recommended Action

Verify the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

SEC-3008**Message**

Event: <Event Name>, Status: success, Info: FCS member moved from position <Old FCS position> to <New FCS position>.

Message Type

AUDIT

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates the fabric configuration server (FCS) list has been modified. One of the members of the list has been moved to a new position in the list.

Recommended Action

Verify the modification was planned. If the modification was planned, no action is required. If the modification was not planned, take appropriate action as defined by your enterprise security policy.

SEC-3009**Message**

Event: <Event Name>, Status: success, Info: Security Transaction aborted.

Message Type

AUDIT

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates the pending security transaction is aborted.

Recommended Action

Verify the security transaction was intentionally aborted. If the security transaction was intentionally aborted, no action is required. If the security transaction was not intentionally aborted, take appropriate action as defined by your enterprise security policy.

SEC-3010**Message**

Event: <Event Name>, Status: success, Info: Reset [<Name of security stat(s) reset>] security stat(s).

Message Type

AUDIT

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates a user has reset all the security statistics.

Recommended Action

Verify the security statistics were intentionally reset. If the security statistics were intentionally reset, no action is required. If the security statistics were not intentionally reset, take appropriate action as defined by your enterprise security policy.

SEC-3011**Message**

Event: <Event Name>, Status: success, Info: Reset [<Stat name>] statistics on domain(s) [<Domain IDs>].

Message Type

AUDIT

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates a user has reset a security statistic on the specified domains.

Recommended Action

Verify the security statistics were intentionally reset. If the security statistics were intentionally reset, no action is required. If the security statistics were not intentionally reset, take appropriate action as defined by your enterprise security policy.

SEC-3012**Message**

Event: <Event Name>, Status: success, Info: Temp Passwd <Password Set or Reset> on domain [<Domain ID>] for account [<Account name>].

Message Type

AUDIT

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates a user has reset the password for the specified user accounts.

Recommended Action

Verify the password was intentionally reset. If the password was intentionally reset, no action is required. If the password was not intentionally reset, take appropriate action as defined by your enterprise security policy.

SEC-3013**Message**

Event: <Event Name>, Status: success, Info: Security Version stamp is reset.

Message Type

AUDIT

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates a user has reset the security version stamp.

Recommended Action

Verify the security version stamp was intentionally reset. If the security event was planned, no action is required. If the security version stamp was not intentionally reset, take appropriate action as defined by your enterprise security policy.

SEC-3014**Message**

Event: <Event Name>, Status: success, Info: <Event related info> <Security server> server <Server Name> for AAA services.

Message Type

AUDIT

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates a user has changed the RADIUS, LDAP, or TACACS+ configuration.

Recommended Action

Verify the RADIUS configuration was changed intentionally. If the RADIUS configuration was changed intentionally, no action is required. If the RADIUS configuration was not changed intentionally, take appropriate action as defined by your enterprise security policy.

SEC-3015**Message**

Event: <Event Name>, Status: success, Info: Moved <Event option> server <Server name> to position <New position>.

Message Type

AUDIT

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates a user has changed the position of the RADIUS, LDAP, or TACACS+ server.

Recommended Action

Verify the remote server position was intentionally changed. If the remote server position was intentionally changed, no action is required. If the remote server position was not intentionally changed, take appropriate action as defined by your enterprise security policy.

SEC-3016**Message**

Event: <Event Name>, Status: success, Info: Attribute [<Attribute Name>] of <Security server> server <server ID> changed <Attribute related info, if any>.

Message Type

AUDIT

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates a user has changed the specified attribute of the RADIUS, LDAP, and TACACS+ server.

Recommended Action

Verify the RADIUS/LDAP/TACACS+ attribute was intentionally changed. If the RADIUS attribute was intentionally changed, no action is required. If the RADIUS/LDAP/TACACS+ attribute was not intentionally changed, take appropriate action as defined by your enterprise security policy.

SEC-3018

Message

Event: <Event Name>, Status: success, Info: Parameter [<Parameter Name>] changed from [<Old Value>] to [<New Value>].

Message Type

AUDIT

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates the specified password configuration parameter is changed.

Recommended Action

Verify the password configuration parameter was intentionally changed. If the password configuration parameter was intentionally changed, no action is required. If the password configuration parameter was not intentionally changed, take appropriate action as defined by your enterprise security policy.

SEC-3019

Message

Event: <Event Name>, Status: success, Info: Passwdcfg parameters set to default values.

Message Type

AUDIT

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates the password configuration parameters are set to default values.

Recommended Action

Verify the password configuration parameter was intentionally set to default values. If the password configuration parameter was intentionally set to default values, no action is required. If the password configuration parameter was not intentionally set to default values, take appropriate action as defined by your enterprise security policy.

SEC-3020**Message**

Event: <Event Name>, Status: success, Info: Successful login attempt via <connection method and IP Address>.

Message Type

AUDIT

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates a successful login occurred. An IP address is displayed when the login occurs over a remote connection.

Recommended Action

Verify the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

SEC-3021**Message**

Event: <Event Name>, Status: failed, Info: Failed login attempt via <connection method and IP Address>.

Message Type

AUDIT

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates a failed login attempt occurred.

Recommended Action

Verify the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

SEC-3022**Message**

Event: <Event Name>, Status: success, Info: Successful logout by user [<User>].

Message Type

AUDIT

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates the specified user has successfully logged out.

SEC-3023**Message**

Event: <Event Name>, Status: failed, Info: Account [<User>] locked, failed password attempts exceeded.

Message Type

AUDIT

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates that failed password attempts exceeded the allowed limit; the account has been locked.

Recommended Action

The account may automatically unlock after the lockout duration has expired or an administrator may manually unlock the account.

SEC-3024

Message

Event: <Event Name>, Status: success, Info: User account [<User Name>], password changed.

Message Type

AUDIT

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates the user's password was changed.

Recommended Action

Verify the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

SEC-3025

Message

Event: <Event Name>, Status: success, Info: User account [<User Name>] added. Role: [<Role Type>], Password [<Password Expired or not>], Home Context [<Home AD>], AD/VF list [<AD membership List>].

Message Type

AUDIT

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates a new user account was created. In VF mode, when chassis role is added for the user, membership list will include 255.

Recommended Action

Verify the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

SEC-3026**Message**

Event: <Event Name>, Status: success, Info: User account [<User Name>], role changed from [<Old Role Type>] to [<New Role Type>].

Message Type

AUDIT

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates a user account role was changed.

Recommended Action

Verify the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

SEC-3027**Message**

Event: <Event Name>, Status: success, Info: User account [<User Name>] [<Changed Attributes>].

Message Type

AUDIT

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates user account properties were changed.

Recommended Action

Verify the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

SEC-3028**Message**

Event: <Event Name>, Status: success, Info: User account [<User Name>] deleted.

Message Type

AUDIT

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates the specified user account was deleted.

Recommended Action

Verify the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

SEC-3029**Message**

Event: <Event Name>, Status: success, Info: Backup user account \"<User Account Name>\" recovered.

Message Type

AUDIT

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates that backup user accounts were recovered.

Recommended Action

Verify the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

SEC-3030**Message**

Event: <Event Name>, Status: success, Info: <Event Specific Info>.

Message Type

AUDIT

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates the specified `secCertMgmt` operation was performed.

Recommended Action

Verify the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

SEC-3031**Message**

Event: <Event Name>, Status: success, Info: Distributed<List of Databases> db(s) to <Number of domains> domain(s), dom-id(s)<List of Domains>.

Message Type

AUDIT

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates the specified event has occurred.

Recommended Action

Verify the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

SEC-3032**Message**

Event: <Event Name>, Status: success, Info: Switch is configured to <accept or reject> <Database name> database.

Message Type

AUDIT

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates the specified event has occurred to accept or reject a certain database.

Recommended Action

Verify the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

SEC-3033**Message**

Event: fddcfg --fabwideset, Status: success, Info: Fabric wide configuration set to <Fabric-wide configuration set by user>.

Message Type

AUDIT

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates the specified event has occurred.

Recommended Action

Verify the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

SEC-3034**Message**

Event: aaaconfig, Status: success, Info: Authentication configuration changed from <Previous Mode> to <Current Mode> <Existing sessions are terminated or not>.

Message Type

AUDIT

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates an authentication configuration has changed.

Recommended Action

Verify the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

SEC-3035**Message**

Event: ipfilter, Status: success, Info: <IP Filter Policy> ipfilter policy(ies) saved.

Message Type

AUDIT | LOG

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates the specified IP filter policies has been saved.

Recommended Action

Verify the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

SEC-3036**Message**

Event: ipfilter, Status: failed, Info: Failed to save changes for <IP Filter Policy> ipfilter policy(s).

Message Type

AUDIT | LOG

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates the specified IP filter policies have not been saved.

Recommended Action

Verify the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

SEC-3037**Message**

Event: ipfilter, Status: success, Info: <IP Filter Policy> ipfilter policy activated.

Message Type

AUDIT | LOG

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates the specified IP filter policy has been activated.

Recommended Action

Verify the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

SEC-3038**Message**

Event: ipfilter, Status: failed, Info: Failed to activate <IP Filter Policy> ipfilter policy.

Message Type

AUDIT | LOG

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates the specified IP filter policy failed to activate.

Recommended Action

Verify the security event was planned. If the event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

SEC-3039**Message**

Event: Security Violation , Status: failed, Info: Unauthorized host with IP address <IP address of the violating host> tries to establish connection using <Protocol Connection Type>.

Message Type

AUDIT | LOG

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates a security violation was reported. The IP address of the unauthorized host is displayed in the message.

Recommended Action

Check for unauthorized access to the switch through the specified protocol connection.

SEC-3043**Message**

The FIPS inside mode has been set to <Fips Inside>.

Message Type

AUDIT

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates there was a change in the Federal Information Processing Standards (FIPS) Inside mode.

Recommended Action

Verify the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

SEC-3044**Message**

The FIPS mode has been changed to <Fips Mode>.

Message Type

AUDIT

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates there was a change in the Federal Information Processing Standards (FIPS) mode.

Recommended Action

Verify the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

SEC-3045**Message**

Zeroization has been executed on the system.

Message Type

AUDIT

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates the system has been zeroized.

Recommended Action

Verify the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

SEC-3046**Message**

The FIPS Self Tests mode has been set to <Self Test Mode>.

Message Type

AUDIT

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates there was a change in the Federal Information Processing Standards (FIPS) Self Test mode.

Recommended Action

Verify the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

SEC-3047**Message**

Info: RBAC permission for a CLI command: <Cmd Name> is failed.

Message Type

AUDIT

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates the user does not have permission to execute this command.

Recommended Action

Verify the user has the required permission to execute this command.

SEC-3048**Message**

FIPS mode has been enabled in the system using force option.

Message Type

AUDIT

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates the system has been forced to Federal Information Processing Standards (FIPS) mode.

Recommended Action

Verify the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy. Look for the status of the prerequisites that did not conform to FIPS mode.

SEC-3049**Message**

Status of bootprom access is changed using fipscfg CLI to : <Access Status>.

Message Type

AUDIT

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates the status of boot PROM access has changed using the `fipsCfg` command.

SEC-3050**Message**

Event: <Event Name>, Status: success, Info: <Event Specific Info>

Message Type

AUDIT | LOG

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates the specified Secure Shell (SSH) utility operation was performed.

Recommended Action

Verify the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

SEC-3051

Message

The license key/serial number <Key> is <Action>.

Message Type

AUDIT | LOG

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates that a license key is added or removed.

SEC-3061

Message

Role '<Role Name>' is created.

Message Type

AUDIT | LOG

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates that the specified role name has been created.

SEC-3062

Message

Role '<Role Name>' is deleted.

Message Type

AUDIT | LOG

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates that the specified role name has been deleted.

SEC-3063**Message**

Role '<Role Name>' is copied from '<Source Role>'.

Message Type

AUDIT | LOG

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates that the specified role name has been copied from the source role.

SEC-3064**Message**

Permission to the RBAC class(es) '<RBAC Class Names>' is changed for the role '<Role Name>'.

Message Type

AUDIT | LOG

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates the permission to the Role-Based Access Control (RBAC) class is changed for the specified role name.

SEC-3065

Message

Configuration of user-defined roles is uploaded.

Message Type

AUDIT | LOG

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates the configuration of user-defined roles has been uploaded.

SEC-3066

Message

Configuration of user-defined roles is downloaded.

Message Type

AUDIT | LOG

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates the configuration of user-defined roles has been downloaded.

SEC-3067

Message

Invalid Cipher list <Cipher List>.

Message Type

AUDIT | LOG

Message Class

SECURITY

Message Severity

WARNING

Probable Cause

Indicates the input cipher list is an invalid string.

Recommended Action

Invalid cipher list input, therefore reverted to previous cipher list.

SEC-3068**Message**

Self-tests failed on DP. Triggering on CP.

Message Type

AUDIT | LOG

Message Class

SECURITY

Message Severity

WARNING

Probable Cause

Indicates that selftests failed on DP.

Recommended Action

Verify the reason for failure and contact support for further details.

SEC-3069**Message**

Event: seccryptocfg, Status: success, Info: <Action Name> security template, <Template Name>.

Message Type

AUDIT | LOG

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates the specified `seccryptocfg` operation was performed.

Recommended Action

Verify the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

SEC-3070**Message**

Event: <Event Name>, Status: success, Info: Generated self-signed <Certificate Name> certificate, <Certificate Info>.

Message Type

AUDIT | LOG

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates the specified `secCertMgmt` operation was performed.

Recommended Action

Verify the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

SEC-3071**Message**

Event: <Event Name>, Status: success, Info: <Parameter Change Info>.

Message Type

AUDIT

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates the specified password configuration parameter is changed.

Recommended Action

Verify the password configuration parameter was intentionally changed. If the password configuration parameter was intentionally changed, no action is required. If the password configuration parameter was not intentionally changed, take appropriate action as defined by your enterprise security policy.

SEC-3072**Message**

Event: <Event Name>, Status: success, Info: <Event specific info >.

Message Type

AUDIT

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates that the specified Secure Shell (SSH) operation is performed.

Recommended Action

Verify that SSH rekeying is configured and rekeying happened for every configured time interval.

SEC-3073**Message**

Event: <Event Name>, Status: failure, Info: <Event specific info >.

Message Type

AUDIT | LOG

Message Class

SECURITY

Message Severity

WARNING

Probable Cause

Indicates that the specified corrupted or big packet is received in Secure Shell Server (SSHD).

Recommended Action

Verify that the big packet is received in SSHD and SSHD is terminated.

SEC-3074**Message**

<AAA server type> server certificate failed for host name verification.

Message Type

AUDIT | LOG

Message Class

SECURITY

Message Severity

ERROR

Probable Cause

Indicates that RADIUS server certificate failed for host name verification.

SEC-3075**Message**

Event: <Event Name>, <Event action>, Info: <Even specific info >.

Message Type

AUDIT | LOG

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates that unsecure communication service is activated.

Recommended Action

Verify if the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

SEC-3076**Message**

Event: <Event Name>, <Event action>, Info: <Even specific info >.

Message Type

AUDIT | LOG

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates a failure to establish a specified Secure Shell (SSH) session.

Recommended Action

Verify if the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

SEC-3077**Message**

Event: <Event Name>, <Event action>, Info: <Even specific info >.

Message Type

AUDIT | LOG

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates a failure to establish a Transport Layer Security (TLS) session.

Recommended Action

Verify if the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

SEC-3078**Message**

Event: <Event Name>, <Event action>, Info: <Even specific info >.

Message Type

AUDIT

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates TLS session information during connection.

SEC-3079**Message**

Event: Internet Protocol Security (IPsec) is <Event action>.

Message Type

AUDIT | LOG

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates that an Internet Protocol Security (IPsec) or Internet Key Exchange (IKE) policy enabled/disabled and the configuration file was updated.

SEC-3080

Message

Event: Internet Protocol Security (IPsec) configuration is <Event action>, Info: <Even specific info >.

Message Type

AUDIT | LOG

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates that an Internet Protocol Security (IPsec) or Internet Key Exchange (IKE) policy configuration was added/deleted/modified and the configuration file was updated.

SEC-3081

Message

Event: <Event Name>, <Event action>, Info: <Even specific info >.

Message Type

AUDIT | LOG

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates that Transport Layer Security (TLS) Certificate Validation failed.

Recommended Action

Verify if the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

SEC-3082

Message

Telnet session <Session Name> has been closed.

Message Type

AUDIT

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates a user has killed a telnet session.

SEC-3083

Message

<Cfg context> has been updated.

Message Type

AUDIT

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates a user has modified login banner.

SEC-3085

Message

Info: Maintenance permission for a CLI command: <Cmd Name> is failed.

Message Type

AUDIT

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates the user does not have permission to execute this maintenance user command.

Recommended Action

Verify the user has the required permission to execute this maintenance user command.

SEC-3086**Message**

Event :Ldapcfg <Event Name>, Status : <Status>, Info:<Role Name/Role Attributes> <Info String>

Message Type

AUDIT

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates whether ldap role has been mapped/unmapped/changed or not.

Recommended Action

Verify if ldap role has been mapped/unmapped/changed or not.

SEC-3087**Message**

Event: serviceShell <Event Name>, Status: <Status>, Info:<Info String>

Message Type

AUDIT

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates the specified Service Shell utility operation was performed.

Recommended Action

Verify the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

SEC-3088**Message**

Event: <Event Name>, Status: Success, Info: Successful service shell login via <connection method and IP Address>.

Message Type

AUDIT

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates a successful login occurred. An IP address is displayed when the login occurs over a remote connection.

Recommended Action

Verify the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

SEC-3089**Message**

Detected incorrect configuration in <File Name>. Error: <Error string>

Message Type

AUDIT | LOG

Message Class

SECURITY

Message Severity

ERROR

Probable Cause

Failure encountered by monitoring API

Recommended Action

Verify the file for integrity

SEC-3090**Message**

Event: factoryCfg <Event Name>, Status: <Status>, Info:<Info String>

Message Type

AUDIT

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates the specified Factory Cfg utility operation was performed.

Recommended Action

Verify the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

SEC-3091**Message**

Event: <Event Name>, Status: Success, Info: Successful factory shell login via <connection method and IP Address>.

Message Type

AUDIT

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates a successful login occurred. An IP address is displayed when the login occurs over a remote connection.

Recommended Action

Verify the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

SEC-3092**Message**

WWN card programming <Event Name>.

Message Type

AUDIT | LOG

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates the status of programming SEEPROM.

Recommended Action

Verify the event was planned. If the event was planned and successful, no action is required.

SEC-3093**Message**

PEAP 2-factor authentication failure, Falling back to PAP authentication

Message Type

AUDIT | LOG

Message Class

SECURITY

Message Severity

INFO

Probable Cause

PEAP 2-factor authentication failed

Recommended Action**SEC-3094****Message**

Event: <Event Name>, Status: failure, Info: Failed to generate self-signed <Certificate Name> certificate, <Certificate Info>.

Message Type

AUDIT | LOG

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates the specified `secCertMgmt` operation was performed.

Recommended Action

Verify the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

SEC-3095**Message**

Event: <Event Name>, Status: failure, Info: <Event Specific Info>

Message Type

AUDIT | LOG

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates the specified Secure Shell (SSH) utility operation was performed.

Recommended Action

Verify the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

SEC-3096**Message**

Event: IPFilter enforcement, Status: Failed, Info: <Error Message>

Message Type

AUDIT | LOG

Message Class

SECURITY

Message Severity

ERROR

Probable Cause

Indicates that IP filter policy enforcement failed because ipfilter config is not in correct state.

Recommended Action

Execute the **ipfilter --default** to reset the ipfilter configuration to default values.

SEC-3097**Message**

Event: aaaconfig authrconf <Event Name>, Status : <Status>, Info:<Role Name/Role Attributes> <Info String>

Message Type

AUDIT

Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates whether AAA user has been mapped/unmapped/changed or not.

Recommended Action

Verify if AAA user has been mapped/unmapped/changed or not.

SLNK Messages

Support Link module error messages.

SLNK-1001

Message

Supportlink data upload has completed successfully.

Message Type

AUDIT | LOG

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the switch data has been uploaded successfully.

SLNK-1002

Message

Supportlink <config type> configuration updated successfully.

Message Type

AUDIT | LOG

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that "user or profile or default" has updated the supportlink configuration successfully.

SLNK-1003**Message**

Supportlink data collection has completed successfully.

Message Type

AUDIT | LOG

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the switch data has been collected successfully.

SLNK-1005**Message**

Supportlink <failure cmd> failed due to <Error msg> (reason code: <Error code>).

Message Type

AUDIT | LOG

Message Class

CFG

Message Severity

WARNING

Probable Cause

Indicates that supportlink operation failed

SNMP Messages

Simple Network Management Protocol (SNMP) module error messages.

SNMP-1001

Message

SNMP service is not available <Reason>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the Simple Network Management Protocol (SNMP) service could not be started because of the specified reason. Therefore, you will not be able to query the switch through SNMP.

Recommended Action

Verify that the IP address for the Ethernet and Fibre Channel interface is set correctly. If the specified reason is an initialization failure, restart the switch using the `reboot` command.

SNMP-1002

Message

SNMP <Error Details> initialization failed.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the initialization of the SNMP service failed and therefore you will not be able to query the switch through SNMP.

Recommended Action

Restart or power cycle the switch. This will automatically initialize SNMP.

SNMP-1003

Message

Distribution of Community Strings to Secure Fabric failed.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the changes in the SNMP community strings could not be propagated to other switches in the secure fabric.

Recommended Action

Retry changing the SNMP community strings on the primary switch.

SNMP-1004**Message**

Incorrect SNMP configuration.

Message Type

AUDIT | FFDC | LOG

Message Class

CFG

Message Severity

ERROR

Probable Cause

Indicates that the SNMP configuration is incorrect and therefore the SNMP service will not work correctly.

Recommended Action

Change the SNMP configuration to the default using the `snmpConfig --default` command.

SNMP-1005**Message**

SNMP configuration attribute, <Changed attribute>, <String Value>.

Message Type

AUDIT | LOG

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the SNMP configuration has changed. The modified parameter and the old and new parameter values are displayed in the message.

Recommended Action

Execute the `snmpConfig --show` command to view the new SNMP configuration.

SNMP-1006**Message**

<SNMP Configuration group> configuration was reset to default.

Message Type

AUDIT | LOG

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the specified SNMP configuration group was reset to the factory default.

Recommended Action

Execute the `snmpConfig --show` command for the group to view the new SNMP configuration.

SNMP-1009**Message**

Port traps are <blocked state> on port <port>.

Message Type

AUDIT | LOG

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates the blocked or unblocked status of the port traps on the specified port.

Recommended Action

Execute the `snmpTraps --show` command to view the current status of the port.

SNMP-1010

Message

Unsupported security protocol settings detected. Setting SNMP usm privacy protocol configuration to default configuration.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the SNMP User-based Security Model (USM) privacy protocol configuration was found to be incorrect after HA synchronization.

Recommended Action

Execute the `snmpConfig --show` command to view the new SNMP configuration.

SNMP-1011

Message

SNMP configuration attribute, <Changed attribute>, <String Value>.

Message Type

AUDIT | LOG

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the SNMP configuration has been added. The added parameter value is displayed in the message.

Recommended Action

Execute the `snmpConfig --show` command to view the new SNMP configuration.

SNMP-1012**Message**

SNMP configuration attribute, <Changed attribute>, <String Value>.

Message Type

AUDIT | LOG

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the SNMP configuration has been deleted. The deleted parameter value is displayed in the message.

Recommended Action

Execute the `snmpConfig --show` command to view the new SNMP configuration.

SNMP-1013**Message**

Snmpv3 users [<Index>] have authentication and privacy password length less than 8. Please reconfigure it.

Message Type

AUDIT | LOG

Message Class

CFG

Message Severity

WARNING

Probable Cause

Some of the snmpv3 users have authentication and privacy passwords lesser than 8.

Recommended Action

Reconfigure the snmpv3 user authentication and privacy passwords using `snmpconfig --set snmpv3 command`.

SNMP-3020**Message**

Event: Login, Info: SNMP login attempt via <connection method and IP Address>.

Message Type

AUDIT

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates that a simple network management protocol (SNMP) login occurred. An IP address is displayed when the login occurs over a remote connection.

Recommended Action

Verify the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

SPM Messages

Error messages that indicate problems with key or SP management.

SPM-1001**Message**

Init fails: <Reason>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the security processor management (SPM) failed to initialize.

Recommended Action

Check the system resources and restart the switch.

SPM-1002**Message**

Generic SPM Warning: <Reason>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates an security processor management (SPM) warning based on the reason displayed.

Recommended Action

Execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

SPM-1003**Message**

Set New Group Cfg SC Enable <SC_Enable> KV Type <KV_Type>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates a new group has been configured.

SPM-1004**Message**

Initialize Node.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates a node initialization.

SPM-1005**Message**

Set EE Control slot <slot> action <action>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates specified control action is taken on encryption engine in specified slot.

SPM-1006**Message**

Registered Certificate of type <cert_type>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates a certificate registration.

SPM-1007**Message**

Deregistered Certificate cid [<cert_id>] type <cert_type> idx <qc_idx>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates a certificate de-registration.

SPM-1008**Message**

Deregistered SP Certificate in slot <slot>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates an security processor (SP) certificate de-registration.

SPM-1009**Message**

<cert> Certificate is missing.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the specified certificate is missing.

Recommended Action

Execute the `cryptocfg --initnode` command.

SPM-1010**Message**

<cert> Key Vault Certificate is missing.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the specified key vault certificate is missing.

Recommended Action

Deregister and register the key vault.

SPM-1011

Message

Group Cfg Changed Quorum Size <qc_size>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that a group configuration has changed the quorum size.

SPM-1012

Message

Authentication Context: <established>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates an authentication context.

SPM-1013

Message

Security database is out of sync.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates a failure to distribute security database.

Recommended Action

Execute the `cryptocfg --sync -securitydb` command to manually sync the security database.

SPM-1014

Message

Warning: Configdownload may change key vault configuration and result in EE going to Operational; Need Valid KEK state.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates the master keys downloaded will not be effective unless imported because the encryption engine may have different master key configured.

Recommended Action

Import required master keys using the `cryptocfg --recovermasterkey` command to bring the encryption engine online.

SPM-1015

Message

Security database may be out of sync.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates a failure to distribute the security database.

Recommended Action

Use the `cryptocfg --sync -securitydb` command to manually sync security database.

SPM-1016**Message**

Security database is out of sync. This warning can be ignored if the nodes in the EG are running different versions of FOS.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates a failure to distribute the security database.

Recommended Action

Use the `cryptocfg --sync -securitydb` command to manually sync security database.

SPM-3001**Message**

Event: cryptocfg Status: success, Info: Node [<wwnstr>] initialized.

Message Type

AUDIT | LOG

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates a node was initialized.

SPM-3002**Message**

Event: cryptocfg Status: success, Info: EE in slot <slot> initialized.

Message Type

AUDIT | LOG

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates an encryption engine was initialized.

SPM-3003**Message**

Event: cryptocfg Status: success, Info: EE in slot <slot> registered.

Message Type

AUDIT | LOG

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates an encryption engine was registered.

SPM-3004

Message

Event: cryptocfg Status: success, Info: EE in slot <slot> enabled.

Message Type

AUDIT | LOG

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates an encryption engine was enabled.

SPM-3005

Message

Event: cryptocfg Status: success, Info: EE in slot <slot> disabled.

Message Type

AUDIT | LOG

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates an encryption engine was disabled.

SPM-3006

Message

Event: cryptocfg Status: success, Info: <sourceFile> file exported via scp: <hostUsername>[<hostIP>]:<hostPath>.

Message Type

AUDIT | LOG

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates a file was exported through SCP protocol.

SPM-3007**Message**

Event: cryptocfg Status: success, Info: File imported via scp: <hostUsername>[<hostIP>]:<hostPath>.

Message Type

AUDIT | LOG

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates a file was imported through SCP protocol

SPM-3008**Message**

Event: cryptocfg Status: success, Info: DH challenge generated for vault IP <vaultIP>.

Message Type

AUDIT | LOG

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates a DH challenge was generated for a key vault.

SPM-3009

Message

Event: cryptocfg Status: success, Info: DH response accepted.

Message Type

AUDIT | LOG

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates a DH response was accepted.

SPM-3010

Message

Event: cryptocfg Status: success, Info: EE in slot <slot> zeroized.

Message Type

AUDIT | LOG

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates an encryption engine was zeroized.

SPM-3011

Message

Event: cryptocfg Status: success, Info: Local file \"<filename>\" deleted.

Message Type

AUDIT | LOG

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates a locally stored file was deleted.

SPM-3012**Message**

Event: cryptocfg Status: success, Info: <primaryOrSecondary> key vault registered. Certificate label: \"<certLabel>\"
Certificate file: \"<certFilename>\" IP address: <IPAddress>.

Message Type

AUDIT | LOG

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates a key vault was registered.

SPM-3013**Message**

Event: cryptocfg Status: success, Info: Key vault with certificate label \"<certLabel>\" deregistered.

Message Type

AUDIT | LOG

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates a key vault was deregistered.

SPM-3014**Message**

Event: cryptocfg Status: success, Info: Key archive client registered with certificate file \"<certFilename>\".

Message Type

AUDIT | LOG

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates a key archive client (KAC) certificate was registered.

SPM-3015**Message**

Event: cryptocfg Status: success, Info: Key vault type set to <keyVaultType>.

Message Type

AUDIT | LOG

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates the key vault type was set.

SPM-3016**Message**

Event: cryptocfg Status: success, Info: Master key generated.

Message Type

AUDIT | LOG

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates a master key was generated

SPM-3017

Message

Event: cryptocfg Status: success, Info: Master key exported.

Message Type

AUDIT | LOG

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates a master key was exported.

SPM-3018

Message

Event: cryptocfg Status: success, Info: <currentOrAlternate> master key recovered.

Message Type

AUDIT | LOG

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates a master key was recovered.

SPM-3019**Message**

Event: cryptotcfg Status: success, Info: System card registered. Certificate label: \"<certLabel>\" Certificate file: \"<certFilename>\".

Message Type

AUDIT | LOG

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates a system card was registered.

SPM-3020**Message**

Event: cryptotcfg Status: success, Info: System card with certificate label \"<certLabel>\" deregistered.

Message Type

AUDIT | LOG

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates a system card was deregistered.

SPM-3021

Message

Event: cryptocfg Status: success, Info: Authentication card registered. Certificate label: \"<certLabel>\" Certificate file: \"<certFilename>\".

Message Type

AUDIT | LOG

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates an authentication card was registered.

SPM-3022

Message

Event: cryptocfg Status: success, Info: Authentication card with certificate label \"<certLabel>\" deregistered.

Message Type

AUDIT | LOG

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates an authentication card was deregistered.

SPM-3023

Message

Event: cryptocfg Status: success, Info: System card <enabledOrDisabled>.

Message Type

AUDIT | LOG

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates use of the system card was enabled or disabled.

SPM-3024**Message**

Event: cryptocfg Status: success, Info: Quorum size set to <quorumsize>.

Message Type

AUDIT | LOG

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates the quorum size was set.

SPM-3025**Message**

Event: cryptocfg Status: success, Info: File imported via USB: Source: <sourcePath> Destination: <destinationFilename>.

Message Type

AUDIT | LOG

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates a file was imported through a USB device.

SPM-3026

Message

Event: cryptocfg Status: success, Info: File exported via usb: Source: <sourcePath> Destination: <destinationFilename>.

Message Type

AUDIT | LOG

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates a file was exported through a USB device

SPM-3027

Message

Event: cryptocfg Status: success, Info: Recovery card registered. Certificate label: \"<certLabel>\" Certificate file: \"<certFilename>\".

Message Type

AUDIT | LOG

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates a recovery card was registered.

SPM-3028

Message

Event: SPM-EE state changed, Info: EE State: <EE Status>.

Message Type

AUDIT | LOG

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates an encryption engine state has changed.

SPM-3029**Message**

Event: KeyVault Connection Status: <status>, Info: KAC_Connect: <kac status>.

Message Type

AUDIT | LOG

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates the status of key vault.

SRM Messages

SRM module error messages.

SRM-1001**Message**

System is alive.

Message Type

AUDIT

Message Class

RAS

Message Severity

INFO

Probable Cause

Indicates that the system is alive.

SRM-1001**Message**

System is alive.

Message Type

AUDIT

Message Class

RAS

Message Severity

INFO

Probable Cause

Indicates that the system is alive.

SRM-1002**Message**

raslog keep alive period has been changed to <printf>.

Message Type

LOG | AUDIT

Message Class

RAS

Message Severity

INFO

Probable Cause

Indicates that raslog keep alive period has been changed.

SRM-1002**Message**

raslog keep alive period has been changed to <printf>.

Message Type

LOG | AUDIT

Message Class

RAS

Message Severity

INFO

Probable Cause

Indicates that raslog keep alive period has been changed.

SRM-2001**Message**

Management Port Tracker Config Update - <Configuration Parameters and Values>

Message Type

AUDIT | LOG

Message Severity

INFO

Probable Cause

Indicates that Management Port Tracker configuration is updated.

Recommended Action

No Action is required.

SRM-2001**Message**

Management Port Tracker Config Update - <Configuration Parameters and Values>

Message Type

AUDIT | LOG

Message Severity

INFO

Probable Cause

Indicates that Management Port Tracker configuration is updated.

Recommended Action

No Action is required.

SS Messages

The `supportSave` command generates these error messages if problems are encountered.

SS-1000

Message

`supportSave` has uploaded support information to the remote host <Time_Duration>

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the `supportSave` command was used to transfer support information to a remote location.

SS-1001

Message

`supportSave`'s upload operation to remote host has been aborted (<Abort reason>).

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that a file copy error occurred during execution of the `supportSave` command. Complete error information cannot always be displayed in this message because of possible errors in subcommands being executed by the `supportSave` command.

Recommended Action

Check and correct the remote server settings and configuration. Execute the `supportFtp` command (as needed) to set the FTP or SCP parameters. After the problem is corrected, execute the `supportSave` command again.

SS-1002

Message

supportSave has stored support information to the USB storage device.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the `supportSave` command was used to transfer support information to an attached USB storage device.

SS-1003

Message

supportSave's operation to USB storage device aborted.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that a USB operation error occurred during execution of the `supportSave` command. Complete error information cannot always be displayed in this message because of possible errors in subcommands being executed by the `supportSave` command.

Recommended Action

Execute the `usbstorage -l` command to check the USB storage device settings. After the USB problem is corrected, execute the `supportSave` command again.

SS-1004

Message

One or more modules timed out during supportsave. Retry supportsave with -t option to collect all logs.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates a timeout in modules during the execution of the `supportSave` command.

Recommended Action

Execute the `supportSave -t [2-5]` command to collect all logs.

SS-1005**Message**

supportsave failed for the slot <Slot Number>. Reason: No IP connection.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that there is no IP connection between the active control processor (CP) and the blade in the specified slot.

Recommended Action

Check for the IP connection between the active CP and the blade in the specified slot. After the IP connection is established, execute the `supportSave` command again.

SS-1006**Message**

supportsave not collected for slot <Slot Number>. Reason: blade was not available to accept a supportsave request.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the supportsave request was not sent to the blade in the specified slot.

Recommended Action

Restart the switch using the `reboot` command and then execute the `supportSave` command.

SS-1007**Message**

supportsave failed for the slot <Slot Number>. Reason: No response from the blade in the specified slot for the given supportsave request.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that there was no response from the blade in the specified slot for the given supportsave request.

Recommended Action

Restart the switch using the `reboot` command and then execute the `supportSave` command.

SS-1008**Message**

supportsave failed for the slot <Slot Number>. Reason: BP supportsave timeout.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the specified slot has taken more time than expected to collect the supportsave logs.

Recommended Action

Execute the `supportSave` command again.

SS-1009

Message

<slot number and its node name(BP/DP)> supportsave failed. Reason:No ISC connection for <slot number and its node name(BP/DP)>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that there is no Inter-Subsystem Communication (ISC) connection for the specified node slot.

Recommended Action

Restart the switch using the `reboot` command and then execute the `supportSave` command.

SS-1010

Message

CORE/FFDC files have been uploaded to the remote host.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the `supportSave` command was used to transfer core and first failure data capture (FFDC) files to a remote location.

SS-1011

Message

CORE/FFDC files have been transferred to the USB storage device.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the `supportSave` command was used to transfer core and first failure data capture (FFDC) files to a USB storage Device.

SS-1012**Message**

BP supportsave failed. The /mnt of Active CP does not have enough disk space to collect BP supportsave files.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that a chassis with the blade processor (BP) does not have enough disk space in the secondary partition of the active CP to save the supportsave files, before uploading them to the remote host.

Recommended Action

Manually clean up the secondary partition of the active CP to collect the supportsave files.

SS-1013**Message**

supportSave's upload operation aborted. username or password is not provided.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the username or password parameters were not specified with the `supportSave` command in non-interactive mode.

Recommended Action

Specify both username and password or neither of them. If no username and password are specified, anonymous FTP will be used to collect the supportsave files.

SS-1014

Message

supportSave has uploaded information to the remote host(fabos is not ready).

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the `supportSave` command was used to transfer support information to a remote location.

SS-1015

Message

supportSave started.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the `supportSave` command was started to transfer support information to a remote location.

SS-1016

Message

supportSave fails to upload <printf>: <printf>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the `supportSave` command was started to transfer support information to a remote location. And the upload server is temporarily busy to upload a file.

Recommended Action

`supportSave` will retry the upload, no action is required.

SSLP Messages

SSLP module error messages.

SSLP-1001

Message

Failed to launch open source process Service Location Protocol (SLP) in the switch.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that there is an error in launching open source process Service Location Protocol (SLP) in the switch.

Recommended Action

Launch the process manually using the `slpd -d -p /tmp/slpd.pid` command. If this operation fails, reload or fail over the switch.

SULB Messages

Software upgrade library module error messages.

SULB-1001

Message

Firmware download command has started. (From v<current_version> To v<new_version>).

Message Type

AUDIT | LOG

Message Class

FIRMWARE

Message Severity

WARNING

Probable Cause

Indicates that the `firmwareDownload` command has been entered. This process should take approximately 17 minutes. The process is set to time out after 30 minutes.

Recommended Action

Do not fail over or power down the system during firmware upgrade. Allow the `firmwareDownload` command to continue without disruption. No action is required.

Run the `firmwareDownloadStatus` command for more information.

SULB-1002**Message**

Firmwaredownload command has completed successfully.

Message Type

AUDIT | LOG

Message Class

FIRMWARE

Message Severity

INFO

Probable Cause

Indicates that the `firmwareDownload` command has completed successfully and switch firmware has been updated.

Recommended Action

No action is required. The `firmwareDownload` command has completed as expected.

Run the `firmwareDownloadStatus` command for more information. Run the `firmwareShow` command to verify the firmware versions.

SULB-1003**Message**

Firmwarecommit has started.

Message Type

AUDIT | LOG

Message Class

FIRMWARE

Message Severity

INFO

Probable Cause

Indicates that the `firmwareCommit` command has been entered.

Recommended Action

No action is required. Run the `firmwareDownloadStatus` command for more information.

SULB-1004

Message

Firmwarecommit has completed.

Message Type

AUDIT | LOG

Message Class

FIRMWARE

Message Severity

INFO

Probable Cause

Indicates that the `firmwareCommit` command has completed successfully.

Recommended Action

No action is required. Run the `firmwareDownloadStatus` command for more information.

SULB-1005

Message

Current Active CP is preparing to failover.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the active control processor (CP) is about to reboot. The standby CP is taking over as the active CP.

Recommended Action

No action is required. The `firmwareDownload` command is progressing as expected.

Run the `firmwareDownloadStatus` command for more information.

SULB-1006**Message**

Forced failover succeeded. New Active CP is running new firmware.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the previous standby control processor (CP) has now become the active CP and is running the new firmware version.

Recommended Action

No action is required. The `firmwareDownload` command is progressing as expected.

Run the `firmwareDownloadStatus` command for more information.

SULB-1007**Message**

Standby CP reboots.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the standby control processor (CP) is rebooting with new firmware.

Recommended Action

No action is required. The `firmwareDownload` command is progressing as expected.

Run the `firmwareDownloadStatus` command for more information.

SULB-1008

Message

Standby CP booted successfully with new firmware.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the standby control processor (CP) has rebooted successfully.

Recommended Action

No action is required. The `firmwareDownload` command is progressing as expected.

Run the `firmwareDownloadStatus` command for more information.

SULB-1009

Message

Firmwaredownload command failed. Status: 0x<status code>, error: 0x<error code>.

Message Type

AUDIT | LOG

Message Class

FIRMWARE

Message Severity

INFO

Probable Cause

Indicates that the `firmwareDownload` command failed. The additional *status code* and *error code* values provide debugging information.

The following table lists `firmwareDownload` status messages and status codes. Some of them will not be displayed in this RASLog message and are listed for completeness.

Table 8: Status messages and status codes

Status message	Status code
"Firmware download sanity check failed."	0x30
"Sanity check failed because system is non-redundant."	0x31
"Sanity check failed because firmware download is already in progress."	0x32
"Sanity check failed because Fabric OS is disabled on active CP."	0x33
"Sanity check failed because HAMD is disabled on active CP."	0x34
"Sanity check failed because firmware download process is already in progress."	0x35
"Sanity check failed because Fabric OS is disabled on standby CP."	0x36
"Sanity check failed because HAMD is disabled on standby CP."	0x37
"Firmware download failed on standby CP."	0x40
"Firmware download failed on standby CP."	0x41
"Firmware download failed on standby CP."	0x42
"Firmware commit failed on standby CP."	0x43
"Firmware download failed."	0x44
"Firmware download failed due to IPC error."	0x50
"Unable to check the firmware version on standby CP due to IPC error."	0x51
"Firmware download failed due to IPC error."	0x52
"Firmware download failed due to IPC error."	0x53
"Standby CP failed to reboot due to IPC error."	0x54
"Firmware commit operation failed due to IPC error."	0x55
"Unable to check the firmware version on standby CP due to IPC error."	0x56
"Unable to restore the original firmware due to standby CP timeout."	0x57
"Standby CP failed to reboot and was not responding."	0x58
"Unable to check the firmware version on standby CP due to IPC error."	0x59
"Sanity check failed because the firmware download operation is already in progress."	0x60
"Sanity check failed because the firmware download operation is already in progress."	0x61
NOT USED	0x62
"System error."	0x63
"Active CP forced failover succeeded. Now the standby CP becomes active CP."	0x64

Status message	Status code
"Standby CP booted up."	0x65
"Active and standby CP failed to gain HA synchronization within 10 minutes."	0x66
"Standby CP rebooted successfully."	0x67
"Standby CP failed to reboot."	0x68
"Firmware commit has started to restore the secondary partition."	0x69
"Local CP is restoring its secondary partition."	0x6a
"Unable to restore the secondary partition. Run the <code>firmwareDownloadStatus</code> and <code>firmwareShow</code> commands to see firmware status."	0x6b
"Firmware download has started on standby CP. It might take up to 10 minutes."	0x6c
"Firmware download has completed successfully on standby CP."	0x6d
"Standby CP reboots."	0x6e
"Standby CP failed to boot up."	0x6f
"Standby CP booted up with new firmware."	0x70
"Standby CP failed to boot up with new firmware."	0x71
"Firmware download has completed successfully on standby CP."	0x72
"Firmware download has started on standby CP. It might take up to 10 minutes. "	0x73
"Firmware download has completed successfully on standby CP."	0x74
"Standby CP reboots."	0x75
"Standby CP failed to reboot."	0x76
"Firmware commit has started on standby CP."	0x77
"Firmware commit has completed successfully on standby CP."	0x78
"Standby CP booted up with new firmware."	0x79
"Standby CP failed to boot up with new firmware."	0x7a
"Firmware commit has started on both active and standby CPs."	0x7b
"Firmware commit has completed successfully on both active and standby CPs."	0x7c
"Firmware commit failed on active CP."	0x7d
"The original firmware has been restored successfully on standby CP."	0x7e
"Unable to restore the original firmware on standby CP."	0x7f
"Standby CP reboots."	0x80
"Standby CP failed to reboot."	0x81
"Standby CP booted up with new firmware."	0x82
"Standby CP failed to boot up with new firmware."	0x83

Status message	Status code
"There was an unexpected reboot during the firmware download operation. The command is aborted."	0x84
"Standby CP was not responding. The command is aborted."	0x85
"Firmware commit has started on both active and standby CPs. Run the <code>firmwareDownloadStatus</code> and <code>firmwareShow</code> commands to see the firmware status."	0x86
"Firmware commit has started on the local CP. Run the <code>firmwareDownloadStatus</code> and <code>firmwareShow</code> commands to see the firmware status."	0x87
"Firmware commit has started on the remote CP. Run the <code>firmwareDownloadStatus</code> and <code>firmwareShow</code> commands to see the firmware status."	0x88
"Run the <code>firmwareDownloadStatus</code> and <code>firmwareShow</code> commands to see the firmware status."	0x89
"The <code>firmwareDownload</code> command has completed successfully."	0x8a
"The original firmware has been restored successfully."	0x8b
"Remote CP is restoring its secondary partition."	0x8c
"Local CP is restoring its secondary partition."	0x8d
"Remote CP is restoring its secondary partition."	0x8e
"Firmware download has started."	0x8f
"Firmware commit has started."	0x90
"Firmware download has completed successfully."	0x91
"Firmware commit has completed successfully."	0x92
"Firmware commit has started to restore the secondary partition."	0x93
"Firmware commit failed."	0x94
"The secondary partition has been restored successfully."	0x95
"Firmware is being downloaded to the blade. This step may take up to 10 minutes."	0xa0
"Firmware download timed out."	0xa1
"Reboot occurred during firmware download. Firmware commit will be started to recover the blade."	0xa2
"Blade rebooted during firmware commit. The operation will be restarted."	0xa3
"Firmware has been downloaded successfully. Blade is rebooting with the new firmware."	0xa4
"Blade has rebooted successfully."	0xa5
"New firmware failed to boot up. Run the <code>firmwareDownload</code> command again."	0xa6
"Firmware commit has started on the blade. This may take up to 10 minutes."	0xa7

Status message	Status code
"The <code>firmwareRestore</code> command is entered. System will reboot and a firmware commit operation will start upon bootup."	0xa8
"Switch is relocating the AP image."	0xa9
"The AP image is relocated successfully."	0xaa
"Switch reboots during relocating the AP image. The operation will be restarted."	0xab
"Blade failed to reboot with the original image. The <code>firmwareRestore</code> command failed."	0xac

The following table lists additional `firmwareDownload` error messages and error codes. The error code provide more details on the reason for firmware download failure.

Table 9: Error messages and error codes

Error message	Error code
"Image is up-to-date. No need to download the same version of firmware."	0xF
"Upgrade is inconsistent."	0x10
"OSRootPartition is inconsistent. For example: swap OSRootPartitions and reboot."	0x11
"Unable to access the required package list file. Check whether the switch is supported by the requested firmware. Also check the <code>firmwareDownload</code> help page for other possible failure reasons."	0x12
"The RPM package database is inconsistent. Contact your switch service provider for recovery."	0x13
"Out of memory."	0x14
"Failed to download RPM package."	0x15
"Unable to create firmware version file."	0x16
"Unexpected system error."	0x17
"Error in getting lock device for firmware download."	0x18
"Error in releasing lock device for firmware download."	0x19
"Firmware commit failed."	0x1a
"Firmware directory structure is not compatible. Check whether the firmware is supported on this platform."	0x1b
"Failed to load the Linux kernel image."	0x1c
"OSLoader is inconsistent."	0x1d
"New image has not been committed. Run the <code>firmwareCommit</code> or <code>firmwareRestore</code> command and then run the <code>firmwareDownload</code> command."	0x1e
"Firmware restore failed."	0x1f
"Both images are mounted to the same device."	0x20

Error message	Error code
"Unable to uninstall old packages."	0x21
"Firmware download is already in progress."	0x22
"Firmware download timed out."	0x23
"Out of disk space."	0x24
"Primary filesystem is inconsistent. Run the <code>firmwareRestore</code> command to restore the original firmware, or contact your switch service provider for recovery."	0x25
"The post-install script failed."	0x26
"Unexpected reboot."	0x27
"Primary kernel partition is inconsistent. Contact your switch service provider for recovery."	0x28
"The pre-install script failed."	0x29
"The platform option is not supported."	0x2a
"Failed to install RPM package."	0x2b
"Cannot downgrade directly to this version. Downgrade to an intermediate version and then download the desired version."	0x2c
"Invalid RPM package. Reload firmware packages on the file server."	0x2e
"Cannot downgrade due to presence of blade type 17. Remove or power off these blades before proceeding."	0x2f
"Cannot downgrade due to presence of blade type 24. Remove or power off these blades before "	0x30
"Cannot downgrade due to presence of long-distance ports in LS mode. Remove these settings before proceeding."	0x31
"Network is not reachable. Verify the IP address of the server is correct."	0x32

The following descriptions explain the causes of some common error messages:

- 0x15 - "Failed to download RPM package." If this error occurs immediately after firmware download is started, the firmware on the switch may be two releases older than the requested firmware. The firmware download operation supports firmware upgrades within two feature releases (a feature release is indicated by a major number and a minor number; for example, X.Y). In this case, you will need to upgrade to an intermediate version before downloading the desired version. If this error occurs in the middle of a firmware download, the firmware in the file server may be

corrupted or there may be a temporary network issue. In this case, retry the `firmwareDownload` command. If the problem persists, contact your system administrator.

- 0x18 - "Error in getting lock device for firmware download". This error can be due to another firmware download is already in progress. Run the `firmwareDownloadStatus` command to verify that this is the case. Wait for the current session to finish before proceeding.
- 0x23 - "Firmware download timed out." This error may occur because the `firmwareDownloadStatus` command has not completed within the predefined timeout period. It is most often caused by network issues. If the problem persists, contact your system administrator.
- 0x24 - "Out of disk space." This error may occur because some core dump files have not been removed from the filesystem and are using up disk space. Remove these core dump files by using the `supportSave` command before proceeding.
- 0x29 - "The pre-install script failed." This error may be caused by an unsupported blade type. Remove or power off the unsupported blades before proceeding.
- 0x2e - "Invalid RPM package." This error may be caused by an inconsistent firmware image loaded on the file server. It may also be caused by temporary networking issues. Reload the firmware packages on the file server and then retry the `firmwareDownload` command. If the problem persists, contact your system administrator.

The following table lists the `firmwareDownload` state names and code values. They indicate where in the `firmwareDownload` process the error occurred.

Table 10: Upgrade state and code value

Upgrade state	Code
SUS_PEER_CHECK_SANITY	0x21
SUS_PEER_FWDL_BEGIN	0x22
SUS_SBY_FWDL_BEGIN	0x23
SUS_PEER_REBOOT	0x24
SUS_SBY_REBOOT	0x25
SUS_SBY_FABOS_OK	0x26
SUS_PEER_FS_CHECK	0x27
SUS_SELF_FAILOVER	0x28
SUS_SBY_FWDL1_BEGIN	0x29
SUS_SELF_FWDL_BEGIN	0x2a
SUS_SELF_COMMIT	0x2b
SUS_SBY_FWC_BEGIN	0x2c
SUS_SBY_COMMIT	0x2d
SUS_SBY_FS_CHECK	0x2e
SUS_ACT_FWC_BEGIN	0x2f
SUS_PEER_RESTORE_BEGIN	0x30
SUS_SBY_RESTORE_BEGIN	0x31
SUS_PEER_FWC_BEGIN	0x32
SUS_PEER_FS_CHECK1	0x33
SUS_FINISH	0x34
SUS_COMMIT	0x35

Recommended Action

Run the `firmwareDownloadStatus` command for more information.

In a modular switch, when the `firmwareDownload` command fails, the command will synchronize the firmware on the two partitions of each CP by starting a firmware commit operation. Wait until this operation completes (about 10 minutes) before attempting another firmware download.

In a modular switch, when the `firmwareDownload` command fails, the two CPs may end up with different versions of firmware and they may not gain high availability (HA) sync. In this case, run the `firmwareDownload -s` command to upgrade the firmware on the standby CP to the same version as the active CP. Then retry the `firmwareDownload` command to download the desired version of firmware onto the CPs.

Refer to the *Fabric OS Troubleshooting Guide* for troubleshooting information.

SULB-1010**Message**

Firmwarecommit failed (status=0x<error code>).

Message Type

AUDIT | LOG

Message Class

FIRMWARE

Message Severity

INFO

Probable Cause

Indicates that the `firmwareCommit` command failed. The error code provides debugging information.

Recommended Action

If the failure is caused by an inconsistent filesystem, contact your switch service provider.

SULB-1011**Message**

Firmwaredownload command failed. <error string>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the `firmwareDownload` command failed. The *error string* value indicates the reason for failure.

Recommended Action

Run the `firmwareDownloadStatus` command for more information.

Refer to the *Fabric OS Troubleshooting Guide* for troubleshooting information.

SULB-1017**Message**

Firmwaredownload failed in slot <Slot number>.

Message Type

AUDIT | LOG

Message Class

FIRMWARE

Message Severity

ERROR

Probable Cause

Indicates that the `firmwareDownload` command failed on the specified blade. The error may be caused by the inconsistent application processor (AP) blade firmware stored on the active CP. It may also be caused by an internal Ethernet issue or by a persistent storage hardware failure.

Recommended Action

Run the `slotShow` command. If the blade is in the FAULTY state, run the `slotPowerOff` and `slotPowerOn` commands to trigger another firmware download. If the blade is stuck in the LOADING state, remove and re-insert the blade to trigger another firmware download. If the problem persists, contact your switch service provider.

SULB-1018**Message**

Firmwaredownload timed out in slot <Slot number>.

Message Type

AUDIT | LOG

Message Class

FIRMWARE

Message Severity

ERROR

Probable Cause

Indicates that there may be error caused by the blade initialization issue after the new firmware is downloaded and the blade is rebooted. The error may also be caused by an internal Ethernet issue or by a persistent storage hardware failure.

Recommended Action

Run the `slotShow` command. If the blade is in the FAULTY state, run the `slotPowerOff` and `slotPowerOn` commands to trigger another firmware download to the blade. If the blade is stuck in the LOADING state, remove and re-insert the blade to trigger another firmware download. If the problem persists, contact your switch service provider.

SULB-1020**Message**

New firmware failed to boot in slot <Slot number>.

Message Type

AUDIT | LOG

Message Class

FIRMWARE

Message Severity

ERROR

Probable Cause

Indicates that the BP blade is still running the old image even though it should reboot with the new image. This error may indicate that the new image has not been loaded correctly to the specified blade.

Recommended Action

Run the `slotShow` command. If the blade is in a FAULTY state, run the `slotPowerOff` and `slotPowerOn` commands to trigger another firmware download to the blade. If the blade is stuck in LOADING state, remove and re-insert the blade to trigger another firmware download. If the problem persists, contact your switch service provider.

SULB-1021**Message**

Firmware is being downloaded to the blade in slot <Slot number>.

Message Type

AUDIT | LOG

Message Class

FIRMWARE

Message Severity

WARNING

Probable Cause

Indicates that the firmware is being loaded to the specified blade.

Recommended Action

Run the `firmwareDownloadStatus` command to monitor the firmware download progress. After it finishes, run the `firmwareShow` command to verify the firmware versions.

SULB-1022**Message**

The blade in slot <Slot number> has rebooted successfully with new firmware.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the blade in the specified slot has rebooted with new firmware. This is a normal step in the firmware download process.

Recommended Action

Run the `firmwareDownloadStatus` command to monitor the firmware download progress.

SULB-1023**Message**

The blade in slot <Slot number> has rebooted during firmwaredownload.

Message Type

AUDIT | LOG

Message Class

FIRMWARE

Message Severity

WARNING

Probable Cause

Indicates that there may be an error caused by an unexpected disruption of the `firmwareDownload` command; for example, powering off and on of the indicated BP blade in the middle of a firmware download. The error may also be caused by persistent storage hardware failure or by a software error.

Recommended Action

The `firmwareCommit` command will be started automatically after the blade boots up to repair the secondary partition. If at the end of the firmware commit, the blade firmware version is still inconsistent with the active CP firmware, firmware download will be restarted automatically on the blade. Run the `firmwareDownloadStatus` command to monitor the progress. If the problem persists, contact your switch service provider.

SULB-1024**Message**

Firmware commit has completed on the blade in slot <Slot number>.

Message Type

AUDIT | LOG

Message Class

FIRMWARE

Message Severity

WARNING

Probable Cause

Indicates that the `firmwareCommit` command has completed on the specified blade.

Recommended Action

Run the `firmwareShow` command to verify the firmware versions. If the blade firmware is the same as the active CP firmware, the `firmwareDownload` command has completed successfully on the blade. However, if the firmware commit operation has been started to repair the secondary partition, at the end of the firmware commit, the blade firmware version may still be inconsistent with the active CP firmware. In this case, firmware download will automatically be restarted on the blade. Run the `firmwareDownloadStatus` command to monitor the progress.

SULB-1025**Message**

The blade in slot <Slot number> will reboot with the new firmware.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that new firmware has been downloaded to the specified application processor (AP) blade and the AP blade will reboot to activate it.

Recommended Action

Wait for the blade to reboot.

SULB-1026**Message**

Firmware commit operation started on the blade in slot <Slot number>.

Message Type

AUDIT | LOG

Message Class

FIRMWARE

Message Severity

WARNING

Probable Cause

Indicates that the `firmwareCommit` command has started on the specified blade. The operation may be a normal part of firmware download, or it may have started to repair the secondary partition of the blade if the secondary partition is corrupted.

Recommended Action

Wait for the firmware commit operation to complete.

SULB-1030**Message**

The switch has rebooted during relocating the internal firmware image.

Message Type

AUDIT | LOG

Message Class

FIRMWARE

Message Severity

WARNING

Probable Cause

Indicates that there may be an error caused by an unexpected disruption of the `firmwareDownload` command; for example, by powering the switch off and on in the middle of a firmware download. The error may also be caused by persistent storage hardware failure or by a software error.

Recommended Action

The `firmwareDownload` command will continue after the switch has rebooted. Run the `firmwareDownloadStatus` command to monitor progress. If the problem persists, contact your switch service provider.

SULB-1031**Message**

The switch is relocating an internal firmware image.

Message Type

AUDIT | LOG

Message Class

FIRMWARE

Message Severity

WARNING

Probable Cause

Indicates that the switch has rebooted with the new firmware and is relocating the application processor (AP) firmware.

Recommended Action

Wait for the operation to complete.

SULB-1032**Message**

Relocating an internal firmware image on the CP.

Message Type

AUDIT | LOG

Message Class

FIRMWARE

Message Severity

WARNING

Probable Cause

Indicates that the switch has started firmware download to the co-CPU.

Recommended Action

Wait for the operation to complete.

SULB-1033**Message**

Switch has completed relocating the internal firmware image.

Message Type

AUDIT | LOG

Message Class

FIRMWARE

Message Severity

WARNING

Probable Cause

Indicates that the firmware download process has completed normally on the switch.

Recommended Action

Run the `firmwareShow` command to verify the firmware versions. Run the `switchShow` command to make sure the switch is enabled.

SULB-1034**Message**

Relocation of internal image timed out.

Message Type

AUDIT | LOG

Message Class

FIRMWARE

Message Severity

ERROR

Probable Cause

Indicates that there may be an error caused by the switch initialization issue after the internal image is relocated. It may also be caused by an internal Ethernet issue or by a persistent storage hardware failure.

Recommended Action

Reboot the switch. This will cause the internal image to be relocated again. Use the `firmwareDownloadStatus` command to monitor the progress. If the problem persists, contact your switch service provider.

SULB-1035**Message**

An error has occurred during relocation of the internal image.

Message Type

AUDIT | LOG

Message Class

FIRMWARE

Message Severity

ERROR

Probable Cause

Indicates that an error has occurred during the relocation of the internal image. The error may be caused by inconsistent internal firmware image. It may also be caused by an internal Ethernet issue or a persistent storage hardware failure.

Recommended Action

Reset the switch. This will cause the internal image to be relocated again. If the problem persists, contact your switch service provider.

SULB-1036**Message**

<The Version being logged><Version String>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates the version running in the system. This is generally logged before download and after download of the firmware to store version information.

SULB-1037**Message**

HCL failed. Reboot the switch manually using the reboot command. However, it will disrupt the FC traffic.

Message Type

AUDIT | LOG | FFDC

Message Class

FIRMWARE

Message Severity

ERROR

Probable Cause

Indicates that Hot Code Load (HCL) has failed. Many reasons, such as a domain not confirmed, can cause this failure.

Recommended Action

Run the `reboot` command to reboot the switch manually.

SULB-1039**Message**

CP has completed relocating the internal firmware image.

Message Type

AUDIT | LOG

Message Class

FIRMWARE

Message Severity

INFO

Probable Cause

Indicates that the firmware download process has completed normally on the control processor (CP).

Recommended Action

Run the `firmwareShow` command to verify the firmware versions.

SULB-1040**Message**

An error has occurred during relocation of the internal image on the CP.

Message Type

AUDIT | LOG

Message Class

FIRMWARE

Message Severity

WARNING

Probable Cause

Indicates that an error has occurred during the relocation of the internal image. The error may be caused by an inconsistent internal firmware image. It may also be caused by an internal Ethernet failure.

Recommended Action

Run the `firmwareShow` command to verify the firmware versions. Run the `firmwareDownload` command again if the firmware is not updated.

This will cause the internal image to be relocated again. If the problem persists, contact your switch service provider.

SULB-1041**Message**

Firmware has been activated successfully on standby CP.

Message Type

AUDIT | LOG

Message Class

FIRMWARE

Message Severity

INFO

Probable Cause

Indicates that the `firmwareActivate` command has completed successfully on the standby control processor (CP).

Recommended Action

No action is required. The `firmwareActivate` command has completed on the standby CP as expected.

Run the `firmwareShow` command to verify the firmware versions.

SULB-1042**Message**

Firmwareactivate command has completed successfully.

Message Type

AUDIT | LOG

Message Class

FIRMWARE

Message Severity

INFO

Probable Cause

Indicates that the `firmwareActivate` command has completed successfully and the switch firmware has been updated.

Recommended Action

No action is required. The `firmwareActivate` command has completed as expected.

Run the `firmwareShow` command to verify the firmware versions.

SULB-1043**Message**

Firmwareactivate command failed. <error string>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the `firmwareActivate` command failed. The *error string* value indicates the reason for failure.

Recommended Action

Run the `firmwareShow` command to verify the firmware versions.

SULB-1044**Message**

Firmwaredownload to secondary partition has completed successfully.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the `firmwareDownload` command to the secondary partition has completed successfully and the switch will come up with the updated firmware on reboot.

Recommended Action

No action is required. The switch will auto-reboot with the downloaded firmware.

SULB-1050**Message**

Firmwaredownload command continues.

Message Type

AUDIT | LOG

Message Class

FIRMWARE

Message Severity

INFO

Probable Cause

Indicates that the `firmwareDownload` command is running on the standby control processor (CP) of the dual-CP system. This process should take approximately 17 minutes. The process is set to time out after 30 minutes.

Recommended Action

Do not fail over or power down the system during firmware upgrade. Allow the `firmwareDownload` command to continue without disruption. No action is required.

Run the `firmwareDownloadStatus` command for more information.

SULB-1051

Message

Detected hot-plug of Standby CP. Firmware from Active CP will automatically be synchronized to Standby CP.

Message Type

AUDIT | LOG

Message Class

FIRMWARE

Message Severity

INFO

Probable Cause

Indicates that auto firmware synchronization has started because the standby control processor (CP) is hot-plugged.

Recommended Action

No action is required. Firmware download has started on the standby CP.

SULB-1052

Message

Firmwaresync has failed.<return code>

Message Type

AUDIT | LOG

Message Class

FIRMWARE

Message Severity

ERROR

Probable Cause

Indicated that auto firmware synchronization has failed.

Recommended Action

Execute the `firmwareDownloadStatus` and `firmwareShow` commands to view firmware status. Execute the `haShow` command to view the HA state.

SULB-1053

Message

<firmware sync complete>

Message Type

AUDIT | LOG

Message Class

FIRMWARE

Message Severity

INFO

Probable Cause

Indicated that auto firmware synchronization has completed.

SULB-1054

Message

Firmwaresync has started

Message Type

AUDIT | LOG

Message Class

FIRMWARE

Message Severity

INFO

Probable Cause

Indicated that firmware synchronization has started.

SULB-1055

Message

Firmware upgrade on the blade in slot <Slot number> has completed.

Message Type

AUDIT | LOG

Message Class

FIRMWARE

Message Severity

WARNING

Probable Cause

Indicates that the firmware upgrade on the specified blade has completed.

Recommended Action

No action is required. The `firmwareDownload` command has completed as expected.

Run the `firmwareDownloadStatus` command for more information. Run the `firmwareShow` command to verify the firmware versions.

SULB-1056**Message**

Firmware is being downloaded to the blade in slot <Slot number>.

Message Type

AUDIT | LOG

Message Class

FIRMWARE

Message Severity

WARNING

Probable Cause

Indicates that the firmware is being loaded to the specified blade.

Recommended Action

Run the `firmwareDownloadStatus` command to monitor the firmware download progress. After it finishes, run the `firmwareShow` command to verify the firmware versions.

SULB-1060**Message**

Standby CP FOS version (v<major version>.<minor version>.<patch version><patch id>) is below v6.4.0. CP FOS autosync is not permitted.

Message Type

AUDIT | LOG

Message Class

FIRMWARE

Message Severity

WARNING

Probable Cause

Indicates that the control processor (CP) auto firmware synchronization is not permitted.

Recommended Action

Manually run `firmwaredownload` command on the standby CP to synchronize it with the same FOS version as on the active CP.

SULB-1061

Message

TruFOS Certificate validation failed.

Message Type

AUDIT | LOG

Message Class

FIRMWARE

Message Severity

ERROR

Probable Cause

Indicates that firmware upgrade token license validation failed.

Recommended Action

Go to your vendor support site to retrieve a valid TruFOS Certificate.

SULB-1062

Message

Firmwarecleaninstall failed. Please retry firmwarecleaninstall again.

Message Type

AUDIT | LOG

Message Class

FIRMWARE

Message Severity

ERROR

Probable Cause

Firmwarecleaninstall failed due to network error.

Recommended Action

Please retry firmwarecleaninstall again.

SULB-1063

Message

Firmwarepatch installation has completed successfully.

Message Type

AUDIT | LOG

Message Class

FIRMWARE

Message Severity

INFO

Probable Cause

Indicates that the `firmwarepatch --install` command has completed successfully and the switch firmware has been updated.

Recommended Action

No action is required. The `firmwarepatch --install` command has completed as expected.

Run the `firmwarepatch --show` command to verify the patch version installed on the switch.

SULB-1064

Message

Firmwarepatch installation has failed.

Message Type

AUDIT | LOG

Message Class

FIRMWARE

Message Severity

INFO

Probable Cause

Indicates that the `firmwarepatch --install` command failed. The *error string* value indicates the reason for failure.

Recommended Action

None. Internal feature errors are for developers and support teams to fix.

SULB-1065

Message

Firmwarepatch removal has completed successfully.

Message Type

AUDIT | LOG

Message Class

FIRMWARE

Message Severity

INFO

Probable Cause

Indicates that the `firmwarepatch --remove` command has completed successfully and the switch firmware has been updated.

Recommended Action

No action is required. The `firmwarepatch --remove` command has completed as expected.

Run the `firmwarepatch --show` command to verify the patch version installed on the switch.

SULB-1066

Message

Firmwarepatch removal has failed.

Message Type

AUDIT | LOG

Message Class

FIRMWARE

Message Severity

INFO

Probable Cause

Indicates that the `firmwarepatch --remove` command failed. The *error string* value indicates the reason for failure.

Recommended Action

None. Internal feature errors are for developers and support teams to fix.

SULB-1067**Message**

Firmwareactivate command has started...

Message Type

AUDIT | LOG

Message Class

FIRMWARE

Message Severity

INFO

Probable Cause

Indicates that the `firmwareActivate` command has started.

SWCH Messages

SWCH module error messages.

SWCH-1001**Message**

Switch is not in ready state - Switch enable failed, switch status= 0x<switch status>, c_flags = 0x<switch control flags>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the switch is enabled before it is ready.

Recommended Action

If the message persists, execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

SWCH-1002

Message

Security violation: Unauthorized device <wwn name of device> tries to flogin to port <port number>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the specified device is not present in the authorized profile list.

Recommended Action

Verify that the device is authorized to log in to the switch. If the device is authorized, execute the `secPolicyDump` command to verify whether the World Wide Name (WWN) of the specified device is listed. If it is not listed, execute the `secPolicyAdd` command to add this device to an existing policy.

SWCH-1003

Message

Slot ENABLED but Not Ready during recovery, disabling slot = <slot number>(<return value>).

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the slot state has been detected as inconsistent during failover or recovery.

Recommended Action

For a bladed switch, execute the `slotPowerOff` and `slotPowerOn` commands to power cycle the blade.

For a non-bladed switch, reboot or power cycle the switch.

SWCH-1004**Message**

Blade attach failed during recovery, disabling slot = <slot number>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the specified blade has failed during failover or recovery.

Recommended Action

For a bladed switch, execute the `slotPowerOff` and `slotPowerOn` commands to power cycle the blade.

For a non-bladed switch, reboot or power cycle the switch.

SWCH-1005**Message**

Diag attach failed during recovery, disabling slot = <slot number>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the diagnostic blade attach operation has failed during failover or recovery.

Recommended Action

For a bladed switch, execute the `slotPowerOff` and `slotPowerOn` commands to power cycle the blade.

For a non-bladed switch, reboot or power cycle the switch.

SWCH-1006

Message

HA state out of sync: Standby CP (ver = <standby SWC version>) does not support NPIV functionality. (active ver = <active SWC version>, NPIV devices = <'1' if NPIV devices exist; Otherwise '0'>).

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the standby control processor (CP) does not support N_Port ID Virtualization (NPIV) functionality, but the switch has some NPIV devices logged in to the fabric.

Recommended Action

Load a firmware version on a standby CP that supports NPIV functionality using the `firmwareDownload` command.

SWCH-1007

Message

Switch port <port number> disabled due to \"<disable reason>\".

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the switch port is disabled due to the reason displayed in the message.

Recommended Action

Based on the disable reason displayed, take appropriate action to restore the port.

If the disable reason is "Insufficient frame buffers", reduce the distance or speed settings for the port to reduce the buffer requirement of the link. Alternatively, one or more ports in the port group must be disabled to make more buffers available for the link.

Refer to the *Fabric OS Administrator's Guide* for more information.

SWCH-1008

Message

<area string> are port swapped on ports that do not support port swap. Slot <slot number> will be faulted.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the blade enabled with the port configuration that does not support port swap.

Recommended Action

Replace the blade with ports that support port swap. Then swap ports back to the port's default area.

Refer to the *Fabric OS Administrator's Guide* for more information on port swapping.

SWCH-1009

Message

Shared area having Trunk Area (TA) enabled on slot <slot number>. Shared areas that have TA enabled will be persistently disabled.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the blade is enabled with a port configuration that had Trunk Area previously enabled on the shared area port.

Recommended Action

Disable Trunk Area on ports that had Trunk Area enabled previously. Refer to the *Fabric OS Administrator's Guide* for more information.

SWCH-1010

Message

Trunk Area (TA) enabled on slot <slot number> with switch not in PID format 1. TA enabled ports will be persistently disabled.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the blade is enabled with the port configuration that had Trunk Area enabled previously.

Recommended Action

Disable Trunk Area on ports that had Trunk Area enabled previously. Refer to the *Fabric OS Administrator's Guide* for more information.

SWCH-1011

Message

HA out of sync: Stby CP (ver=<standby SWC version>) doesn't support Trunk Area functionality. (active ver=<active SWC version>, TA enabled on sw=<'1' if Trunk Area ports exist; Otherwise '0'>).

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the standby control processor (CP) does not support Trunk Area functionality, but the switch has some ports with Trunk Area enabled.

Recommended Action

Load a firmware version on standby CP that supports Trunk Area functionality by using the `firmwareDownload` command.

SWCH-1012

Message

Trunk Area (<trunk area>) has been enabled for one or more ports.

Message Type

AUDIT | LOG

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that a Trunk Area has been enabled for one or more ports and the configuration file has been updated.

SWCH-1013

Message

Trunk Area has been disabled for one or more ports.

Message Type

AUDIT | LOG

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that a Trunk Area assignment has been disabled for one or more ports and the configuration file has been updated.

SWCH-1014

Message

All Trunk Areas have been disabled.

Message Type

AUDIT | LOG

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that all Trunk Areas have been disabled and the configuration file has been updated.

SWCH-1015**Message**

<Function name> <Description of problem>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that an internal problem has been detected by the software. This is usually an internal Fabric OS problem or due to file corruption.

Recommended Action

Reboot or power cycle the switch.

If the message persists, execute the `firmwareDownload` command to update the firmware.

SWCH-1016**Message**

Device <wwn name of device> FDISC to port <port number>. Static persistent PID set and area requested not assigned to the device. Reject FDISC.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the static persistent port ID (PID) is set and the area requested is not assigned to the device.

Recommended Action

This is an N_Port ID virtualization (NPIV) device and the static persistent PID is set on it, though the area cannot be assigned as requested. Remove the static binding to have the device come up with a different area by using the `wwnaddress --unbind` command.

SWCH-1017**Message**

Device <wwn name of device> tries to FLOGI to port <port number>, reject FLOGI as persistent PID is set on the Loop device.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates persistent port ID (PID) is set and static persistent PID is not supported on loop device.

Recommended Action

Remove the WWN-PID binding using the `wwnaddress --unbind` command and re-enable the port.

SWCH-1018**Message**

Device <wwn name of device> FLOGI to port <port number>, Static persistent PID set, Requested area <area> user bound to another port. Reject FLOGI.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates a WWN-PID and port address binding collision.

Recommended Action

The persistent PID is set on the device and the requested area cannot be assigned because it is user bound to a different port. Remove the WWN-PID binding using the `wwnaddress --unbind` command or remove the port address binding using the `portaddress --unbind` command and then re-enable the port.

SWCH-1019

Message

Device <wwn name of device> tries to FLOGI, reject FLOGI as persistent PID is set on device and port <port number> has user area <area> bound to it.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates a WWN-PID and port address binding collision.

Recommended Action

The persistent PID is set on the device and the requested area cannot be assigned because the port it is trying to log in through has a different area bound to it. Remove the WWN-PID binding using the `wwnaddress --unbind` command or remove the port address binding using the `portaddress --unbind` command and then re-enable the port.

SWCH-1020

Message

HA state out of sync: Standby CP (ver = <standby SWC version>) does not support QoS links to AG(Active CP version = <active SWC version>).

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the standby control processor (CP) does not support links to Access Gateway running quality of service (QoS).

Recommended Action

Load a firmware version on the standby CP that supports QoS links to Access Gateway by using the `firmwareDownload` command.

SWCH-1021

Message

HA state out of sync: Standby CP (ver = <standby SWC version>) does not support Dynamic area on default switch (Active CP version = <active SWC version>).

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the standby control processor (CP) does not support dynamic area on the default switch.

Recommended Action

Load a firmware version on the standby CP that supports dynamic area on the default switch by using the `firmwareDownload` command.

SWCH-1022

Message

Port:<port number> has been disabled due to port address conflict while enabling FMS mode.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the switch has ports with FICON Management Server (FMS) reserved areas (0xFE, 0xFF) that are not supported in FMS mode.

Recommended Action

No action required. Refer to the *FICON Administrator's Guide* for more information.

SWCH-1023

Message

HA state out of sync: Standby CP (ver = <standby SWC version>) does not support XISL use while fmsmode and/or lossless are enabled (Active CP version = <active SWC version>).

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the standby control processor (CP) does not support extended inter-switch link (XISL) while FICON Management Server (FMS) mode and Lossless are enabled.

Recommended Action

Load a firmware version on standby CP that supports both XISL use and FMS mode and Lossless at the same time by using the `firmwareDownload` command.

SWCH-1024**Message**

HA state out of sync: Standby CP (ver = <standby SWC version>) does not support active's enforce_login policy (Active CP version =<active SWC version>).

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the standby control processor (CP) does not enforce login policy of the active CP.

Recommended Action

Configure the enforce login policy to a value that the standby CP supports.

SWCH-1025**Message**

This Logical Switch has 8Gbps-capable FC ports. Edge Hold Time for these ports is unchanged and is <Edge Hold Time>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the edge hold time for the 8 Gbps-capable FC ports is not the same as non 8 Gbps-capable FC ports in the logical switch. The 8 Gbps-capable FC ports use the edge hold time configured on the default switch.

Recommended Action

To know the edge hold time configured for 8 Gbps-capable FC ports, go to the default switch and execute the `configShow` command.

SWCH-1026**Message**

HA state out of sync: Standby CP (ver = <standby SWC version>) does not support auto csctl_mode (Active CP version = <active SWC version>).

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the standby control processor (CP) does not support auto class-specific control (CS_CTL) mode.

Recommended Action

Upgrade the standby CP firmware version to same level as active CP.

SWCH-1027**Message**

HA state out of sync: Standby CP (ver = <standby SWC version>) does not support NPIV Base device Logout functionality. (active ver = <active SWC version>).

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the standby control processor (CP) does not support N_Port ID Virtualization (NPIV) base device logout functionality, but the switch has some ports with base device configured.

Recommended Action

Load a firmware version on standby CP that supports NPIV Base device Logout functionality using the `firmwareDownload` command, or change the 'base logout' feature with the `portCfgNPIVPort` command.

SWCH-1028**Message**

The base FLOGI device(PID: 0x<PID>)) has logged out from the port (Index <Port Index>).

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the FLOGI assigned N_Port logged out from the port and other N_Ports are still active on the port.

SWCH-1029**Message**

supportinfoclear --clear was issued<message>

Message Type

AUDIT

Message Class

CLI

Message Severity

INFO

Probable Cause

Indicates all the default statistics with portlogs and errorlogs are cleared.

SWCH-1030**Message**

Switch port <port number> statistics cleared.

Message Type

AUDIT

Message Class

FABRIC

Message Severity

INFO

Probable Cause

Indicates that the switch port statistics have been cleared.

SWCH-1031**Message**

Port <port number> recovery failed.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that warm recovery for specified port is failed upon high availability (HA).

SWCH-1032**Message**

Error statistics of the ethernet interface <Interface> was cleared.

Message Type

AUDIT | LOG

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates Ethernet management interface error counters are cleared.

SWCH-1033

Message

Ethernet connectivity Speed/Duplexity is configured for interface <Interface> .

Message Type

AUDIT | LOG

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates Ethernet connectivity parameters speed or duplexity are configured.

SWCH-1034

Message

Switch has been enabled.

Message Type

AUDIT

Message Class

CLI

Message Severity

INFO

Probable Cause

Indicates that a switch is being intentionally enabled.

SWCH-1035

Message

Switch has been disabled.

Message Type

AUDIT

Message Class

CLI

Message Severity

INFO

Probable Cause

Indicates that a switch is being intentionally disabled.

SWCH-1036**Message**

Switch has been persistently enabled.

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that a switch is being persistently enabled.

SWCH-1037**Message**

Switch has been persistently disabled.

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that a switch is being persistently disabled.

SWCH-1038

Message

Principal Selection Mode has been enabled, which will be activated from the next fabric rebuild.

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that Principal Switch Selection mode has been enabled, which will be activated from next fabric rebuild .

SWCH-1039

Message

Principal Selection Mode has been enabled, which will force fabric rebuild.

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that Principal Switch Selection mode has been enabled, which will force fabric rebuild .

SWCH-1040

Message

Principal Selection Mode has been disabled.

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that Principal Switch Selection mode has been disabled .

SWCH-1041**Message**

HA state out of sync: Standby CP (ver = <standby SWC version>) does not support FICON Logical Switch. (active ver = <active SWC version>).

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the standby control processor (CP) does not support FICON Logical Switch, but the active switch has a FICON Logical Switch configured..

Recommended Action

Load a firmware version on standby CP that supports FICON Logical Switch functionality using the `firmwareDownload` command, or delete the FICON Logical Switch using `lscfg --delete` command.

SWCH-1042**Message**

Bound address for port (ID: <port number>).

Message Type

AUDIT

Message Class

CLI

Message Severity

INFO

Probable Cause

User has bound address to specified port.

SWCH-1043**Message**

Unbound address for port (ID: <port number>).

Message Type

AUDIT

Message Class

CLI

Message Severity

INFO

Probable Cause

User has unbound address to specified port.

SWCH-1044**Message**

Switch port <port number>. SID:0x<sid>, DID:0x<did>, type:<type> is invalid. OX_ID:0x<OD_ID>

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates fab type is invalid.

SWCH-1045**Message**

Configured NPIV Login Limit of <ConfiguredNPIVLoginLimit> reached on port index <Port>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the current login is the last one that can be allowed on the given port.

Recommended Action

If more NPIV devices are to be added to this port, the Configured NPIV Limit needs to be increased with `portCfgNPIVPort --setloginlimit` command.

SWCH-1046**Message**

Configured NPIV Login Limit of <ConfiguredNPIVLoginLimit> exceeded on port index <Port>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the current login will not be allowed because the configured NPIV Login Limit has been exceeded.

Recommended Action

If more NPIV devices are to be added to this port, the Configured NPIV Limit needs to be increased with `portCfgNPIVPort --setloginlimit` command.

SWCH-1047**Message**

The max limit of NPIV login which both Active and Standby CP can support has been reached for port <port number>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates max limit of NPIV login has been reached in either Active CP or Standby CP for port in blade FC32-48

Recommended Action

Load a firmware version on a standby CP that supports the same max limit of NPIV login as in using the `firmwareDownload` command.

SWCH-1048**Message**

HA state out of sync: Standby CP (ver=<standby SWC version>) does not support the same max limit of NPIV login as in Active CP (ver=<active SWC version>).

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the standby control processor (CP) does not support the same max limit of N_Port ID Virtualization (NPIV) login as in Active CP for the slot port 0-15 in FC32-48 blades

Recommended Action

Load a firmware version on a standby CP that supports the same max limit of NPIV login as in using the `firmwareDownload` command.

SWCH-1049**Message**

Port <port number> cannot accept more NPIV logins because lossless is disabled in the <msg>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates the number of logins allowed in 9-bit area mode has been exceeded and the port cannot be converted to 8-bit area mode to allow further logins because lossless is disabled.

Recommended Action

Enable the lossless in the indicating switch.

SWCH-1050

Message

Switch beacon has been <printf>.

Message Type

AUDIT

Message Class

CLI

Message Severity

INFO

Probable Cause

Indicates that a switch beacon is being enabled/disabled.

SWCH-1051

Message

Trunk Area (<trunk area>) has been enabled for port <port number>.

Message Type

AUDIT | LOG

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that a Trunk Area has been enabled for a port and the configuration file has been updated.

SWCH-1052

Message

Trunk Area (<trunk area>) has been disabled for port <port number>.

Message Type

AUDIT | LOG

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that a Trunk Area has been disabled for a port and the configuration file has been updated.

SWCH-1053**Message**

Port <Port Number> has been disabled; device does not support D-Port functionality.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates a device that does not support D-Port functionality has tried to log in to the D-Port of the switch.

Recommended Action

Configure the D-Port functionality on the device or disable the D-Port configuration. Use the `portcfgdport` command to change the D-Port configuration.

SWCH-1060**Message**

SFP Optics information: <SFP operating msg>.

Message Type

AUDIT | LOG

Message Class

CFG

Message Severity

WARNING

Probable Cause

Indicates SFP optics related information or warnings messages, this may require user attention.

Recommended Action

This may require user to check the optics of this port.

SWCH-1061**Message**

HA state out of sync: Standby CP (ver = <standby SWC version>) is not compatible with Active CP (version =<active SWC version>).

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the standby control processor (CP) is not running a firmware that is compatible with Active Control Processor (CP).

Recommended Action

Load a firmware version on standby CP that is compatible with Active CP by using the `firmwareDownload` command.

SWCH-1062**Message**

Login from <Configured NPIV login limit> rejected on port <Number of logged out WWN-bound PIDs>. NPIV limit of <printf> reached due to <printf> currently unused bound addresses.

Message Type

LOG

Message Severity

WARNING

Probable Cause

WWN based Persistent PID is enabled on the switch and the number of bound WWNs matches the NPIV login limit. Some, but not all, of those bound WWNs are currently logged in. A new WWN attempts to login because the number of actually logged in devices has not yet reached the limit. But since all the possible PIDs are bound already, the login is unexpectedly rejected.

Recommended Action

Compare the output of the `wnaddress --show` command to the output of the `portloginshow` command of the identified port to find unused (i.e. not logged in) bound addresses. If those unused addresses will never login to this port again, use the `wnaddress --unbind` to remove those bindings to make room for new WWNs to login.

SWCH-1063**Message**

Advanced mode is enabled.

Message Type

LOG

Message Severity

INFO

Probable Cause

User enables Advanced mode for Traffic optimiser.

Recommended Action

Advanced mode will be enabled.

SWCH-1064**Message**

Advanced mode is disabled.

Message Type

LOG

Message Severity

INFO

Probable Cause

User disables Advanced mode for Traffic optimiser.

Recommended Action

Advanced mode will be disabled.

SWCH-1065

Message

Maximum number of ports are configured with Application Header for the switch with FID <FID>

Message Type

LOG

Message Severity

INFO

Probable Cause

User configured maximum number of permissible ports with Application Header configuration.

Recommended Action

Disable Application Header Configuration on any of the ports and retry the operation.

SYSC Messages

System Controller daemon error messages.

SYSC-1001

Message

Failed to run <Name of program that could not be run (string)>:<System internal error message (string)>.

Message Type

FFDC | LOG

Message Severity

CRITICAL

Probable Cause

Indicates that one of the programs would not run on the system during the boot sequence.

Recommended Action

If the message is reported during a reboot after new firmware has been loaded, try reloading the firmware using the `firmwareDownload` command.

If the message persists, there may be a conflict between the two versions of firmware or the nonvolatile storage may be corrupted.

If the message persists, execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

SYSC-1002

Message

Switch bring-up timed out.

Message Type

FFDC | LOG

Message Severity

CRITICAL

Probable Cause

Indicates that the system timed out during a reboot or failover sequence, waiting for one or more programs to register with system services or to fail over to active status.

Recommended Action

The switch is in an inconsistent state and can be corrected only by a reboot or power cycle. Before rebooting the chassis, record the firmware version on the switch or control processor (CP) and run the `haDump` command. If this is a dual-CP switch, gather the output from the CP in which this log message appeared.

SYSC-1004

Message

Daemon <Daemon name to restart> restart successful.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that a terminated daemon is restarted by the system automatically.

Recommended Action

Execute the `supportSave` command to gather troubleshooting data. No further action is required.

SYSC-1005

Message

Daemon <Daemon name to restart> is not restarted (Reason: <Restart failure reason>).

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that a terminated daemon is not restarted, either because a restart limit is reached or a restart action fails.

Recommended Action

Execute the `supportSave` command to gather troubleshooting data. Execute the `reboot` or `haFailover` command to recover the system.

SYSM Messages

General system messages.

SYSM-1001

Message

No memory.

Message Type

FFDC | LOG

Message Severity

CRITICAL

Probable Cause

Indicates the switch has run out of system memory.

Recommended Action

Run the `memShow` command to view the switch memory usage.

Reboot or power cycle the switch.

Run the `supportFtp` command (as needed) to set up automatic FTP transfers; then run the `supportSave` command and contact your switch service provider.

SYSM-1002

Message

<number>, Switch: <Switch number>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates a user has executed either the `switchShutdown` or `switchReboot` command. All services are brought down for a logical switch.

Recommended Action

No action is required if the `switchShutdown` or `switchReboot` command was executed intentionally. If the `switchShutdown` command was run, you must run the `switchStart` command to restart traffic on the logical switch.

SYSM-1003**Message**

<number>, Switch: <start reason>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates the user executed the `switchStart` or `switchReboot` command. All services are brought back up after a temporary shutdown of the logical switch.

Recommended Action

No action is required if the `switchStart` command was executed intentionally. Because reinitializing a switch is a disruptive operation and can stop I/O traffic, you may have to stop and restart the traffic during this process.

SYSM-1004**Message**

Failed to retrieve current chassis configuration option, ret=<Unknown>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates there was a failure to read configuration data from the World Wide Name (WWN) card.

Recommended Action

Verify that the WWN card is present and operational and the affected control processor (CP) is properly seated in its slot.

SYSM-1005**Message**

CP blade in slot <Slot number> failed to retrieve current chassis type.

Message Type

FFDC | LOG

Message Severity

CRITICAL

Probable Cause

Indicates there was a failure to read the chassis type from the system.

Recommended Action

Verify the control processor (CP) blade is operational and is properly seated in its slot.

SYSM-1006**Message**

CP blade in slot <Slot number> is incompatible with the chassis type.

Message Type

FFDC | LOG

Message Severity

CRITICAL

Probable Cause

Indicates this chassis type is not compatible with the control processor (CP) blade.

Recommended Action

Use the CP blade on a compatible chassis.

SYSM-1007

Message

PERMITTING USE OF INCOMPATIBLE CHASSIS FOR CP IN SLOT <Slot number>. DATA ERRORS MAY RESULT.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates an override of the incompatible control processor (CP) or chassis check. This message is for engineering use only.

Recommended Action

Delete the /var/chassis_backplane_override file and reboot the CP.

SYSM-1008

Message

RON is set successfully - <roname>

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that Registered Organization Name(RON) is set. This message is for engineering use only.

Recommended Action

None.

TO Messages

Traffic Optimizer module error messages.

TO-1001

Message

Initialization of TO subsystem failed in <File Name>:<Line Number>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the TO subsystem initialization has failed due to internal error.

Recommended Action

Please contact Brocade Support team.

TO-1005

Message

TO Profile <Profile Name> is enforced successfully.

Message Type

AUDIT | LOG

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that specified TO Profile has been enforced.

Recommended Action

No Action is needed.

TO-1006

Message

Flows destined to <DID> device have been moved to <PG Name> PG.

Message Type

LOG

Message Severity

INFO

Probable Cause

The specified Device is over subscribed.

Recommended Action

No Action is needed.

NOTE

Not applicable for FCR flow.

TO-1007**Message**

Flows destined to <DID> device have been moved out of <PG Name> PG.

Message Type

LOG

Message Severity

INFO

Probable Cause

There is no Over subscription condition for the device in last 3 hours.

Recommended Action

No Action is needed.

TO-1008**Message**

Dynamic PG <PG Name> has been created successfully.

Message Type

LOG

Message Severity

INFO

Probable Cause

The specified Performance Group has been created.

Recommended Action

No Action is needed.

TO-1009**Message**

Dynamic PG <PG Name> has been deleted successfully.

Message Type

LOG

Message Severity

INFO

Probable Cause

The Performance Group has been deleted.

Recommended Action**TO-1010****Message**

Link Incompatible mode.

Message Type

LOG

Message Severity

ERROR

Probable Cause**Recommended Action****TO-1011****Message**

Traffic optimizer Profile Mismatch with domain <domain>

Message Type

LOG

Message Severity

WARNING

Probable Cause

TO profile of the switch associated with specified domain is different from the TO profile of the local switch.

Recommended Action

For optimal performance, the TO profile needs to be same across all switches in the fabric. Please consult the user guide to appropriately update the profile.

TO-1012**Message**

HA Sync is stopped because of <Profile_name> <HA_sync_Stop_reason>

Message Type

LOG

Message Severity

ERROR

Probable Cause

HA sync has been stopped due to TO profile incompatibility

Recommended Action

Please refer to the user guide to correct the error.

TO-1013**Message**

System scheduled Profile: <Profile_name> to be activated in 30 days

Message Type

LOG

Message Severity

INFO

Probable Cause

The specified TO profile will be activated in 30 days automatically.

Recommended Action

If user wants to abort it, he/she has to do it within the days mentioned.

TO-1014**Message**

User scheduled Profile: <Profile_name> to be activated in <days> days

Message Type

AUDIT | LOG

Message Class

CFG

Message Severity

INFO

Probable Cause

The specified user scheduled TO profile will be activated in the specified time.

Recommended Action

No Action is needed.

TO-1015**Message**

Scheduled Profile: <Profile_name> will be activated in <days> days

Message Type

LOG

Message Severity

INFO

Probable Cause

TO profile mentioned will be activated in days mentioned automatically.

Recommended Action

If user wants to abort it, he/she has to do it within the days mentioned.

TO-1016

Message

Scheduled Profile: <Profile_name> is aborted

Message Type

AUDIT | LOG

Message Class

CFG

Message Severity

INFO

Probable Cause

User has aborted the previously scheduled profile.

Recommended Action

No Action is needed.

TO-1017

Message

Scheduled Profile: <Profile_name> is aborted due to no Fabric Vision license

Message Type

LOG

Message Severity

INFO

Probable Cause

Migration of TO profile is aborted because of absence of Fabric Vision license.

Recommended Action

Please install Fabric Vision License.

TO-1018

Message

System activated profile <Profile_name> due to no Fabric Vision license

Message Type

LOG

Message Severity

INFO

Probable Cause

Migration of system activated TO profile is aborted because of absence of Fabric Vision license.

Recommended Action

Please install Fabric Vision License.

TO-1019

Message

Profile <Profile_name> cannot be scheduled or activated due to no Fabric Vision license

Message Type

LOG

Message Severity

INFO

Probable Cause

Migration/Activation of TO profile is aborted because of absence of Fabric Vision license.

Recommended Action

Please install Fabric Vision License.

TO-1020

Message

Fabric Vision license removed, on next reboot profile Sys_Trafopt_Version1 will be activated

Message Type

LOG

Message Severity

INFO

Probable Cause

Removal of Fabric Vision license.

Recommended Action

Please install Fabric Vision License if behavior of Sys_Trafopt_Version2 needs to be retained.

TO-3001**Message**

User has updated the Profile <Profile_name> configuration

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

User has updated the custom profile configuration.

Recommended Action

No Action is needed.

TRCE Messages

RAS TRACE error messages.

TRCE-1001**Message**

Trace dump available<slot on which the trace dump occurs>! (reason: <cause of trace dump: PANIC DUMP, WATCHDOG EXPIRED, MANUAL, TRIGGER>).

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that trace dump files have been generated on the switch or the specified slot. The cause for the dump can be one of the following:

- PANICDUMP: Generated by panic dump.
- WATCHDOG EXPIRED: Generated by hardware watchdog expiration.
- MANUAL: Generated manually by issuing the `tracedump -n` command.
- TRIGGER: Triggered by a specific Message ID generated by CRITICAL RASLog message.

Recommended Action

Execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

TRCE-1002**Message**

Trace dump<optional slot indicating on which slot the dump occurs> automatically transferred to address ' <FTP target designated by user> '.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that a trace dump has occurred on the switch or the specified slot, and the trace dump files were automatically transferred from the switch to the specified FTP server.

TRCE-1003**Message**

Trace dump<optional slot indicating on which slot the dump occurs> was not transferred due to FTP error.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that a trace dump has occurred on the switch or the specified slot, but the trace dump files were not automatically transferred from the switch due to reasons such as an FTP error, wrong FTP address, FTP site is down, and network is down.

Recommended Action

Execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

TRCE-1004

Message

Trace dump<slot on which the trace dump occurs> was not transferred because trace auto-FTP disabled.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that trace dump files have been created on the switch or the specified slot, but the trace dump files were not automatically transferred from the switch because auto-FTP is disabled.

Recommended Action

Execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

TRCE-1005

Message

FTP Connectivity Test failed due to error.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the connectivity test to the FTP host failed because of reasons such as a wrong FTP address, FTP site is down, or network is down.

Recommended Action

Execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

TRCE-1006

Message

FTP Connectivity Test succeeded to FTP site ' <FTP target configured by users> '.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that a connectivity test to the FTP host has succeeded.

TRCE-1007**Message**

Notification of this CP has failed. Parameters temporarily out of sync with other CP.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the active control processor (CP) is unable to alert the standby CP of a change in trace status. This message is only applicable to bladed switches.

Recommended Action

This message is often transitory. Wait a few minutes and try the command again.

If the message persists, execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

TRCE-1008**Message**

Unable to load trace parameters.

Message Type

FFDC | LOG

Message Severity

CRITICAL

Probable Cause

Indicates that the active control processor (CP) is unable to read the stored trace parameters.

Recommended Action

Reboot the CP (dual-CP system) or restart the switch.

If the message persists, execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

TRCE-1009**Message**

Unable to alert active CP that a dump has occurred.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the control processor (CP) is unable to communicate trace information to active CP. This message is only applicable to bladed switches.

Recommended Action

Execute the `haShow` command to verify that the current management module is standby and the active management module is active.

If the message persists, execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

TRCE-1010**Message**

Traced fails to start.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the trace daemon (traced), which is used for transferring the trace files has failed to start. The trace capability within the switch is unaffected. The system automatically restarts the traced facility after a brief delay.

Recommended Action

Reboot the CP (dual-CP system) or restart the switch.

If the message persists, execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

TRCE-1011**Message**

Trace dump manually transferred to target ' <optional string to indicate which slot the trace dump is transferred> ': <result>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the trace dump files were transferred manually to the specified slot.

TRCE-1012**Message**

The system was unable to retrieve trace information from slot <Slot number of the interface module on which the attempt was made>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the system was unable to retrieve trace information from the specified slot because there is no communication between the main system and the slot.

Recommended Action

Check that the interface module is enabled and retry the command. If the interface module is already enabled, execute the `supportSave` command and contact your switch service provider.

TRCE-1013

Message

Trace dump <slot on which the trace dump occurs> was not transferred as FIPS mode is enabled.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that a trace dump has occurred on the switch or the specified slot, but the trace dump files were not automatically transferred from the switch because FIPS mode is enabled on the switch.

TS Messages

TS module error messages.

TS-1001

Message

NTP Query failed: <error code>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that a Network Time Protocol (NTP) query to the configured external clock server failed. Local clock time on the principal or primary fabric configuration server (FCS) switch is used for fabric synchronization.

This message may be logged during temporary operational issues such as IP network connection issues to the external clock server. If the message does not recur, it can be ignored.

Recommended Action

Execute the `tsClockServer` command to verify that the configured external clock server is available and functional. If that external clock server is not available, choose another clock server.

TS-1002

Message

<Type of clock server used> used instead of <Type of clock server configured>: locl: 0x<Reference ID of LOCL> remote: 0x<Reference ID of external clock server>.

Message Type

LOG | AUDIT

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates the fabric time synchronization was sourced from an alternate clock server instead of the configured clock server. The clock server used can be one of the following type:

- LOCL - Local clock on the principal or primary FCS switch.
- External - External Network Time Protocol (NTP) server address configured.

This message may be logged during temporary operational issues such as IP network connection issues to the external clock server or the fabric is configured for external time synchronization but the principal or primary fabric configuration server (FCS) does not support the feature. If the message does not recur, it can be ignored.

Recommended Action

Execute the `tsClockServer` command to verify that the principal or primary FCS switch has the clock server IP configured correctly, and the configured clock server is accessible to the switch and functional. If the principal or primary FCS does not support the feature, either choose a different switch for the role or reset the clock server to LOCL.

TS-1006

Message

<message>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that a time service event is occurring or has failed. The message can be one of the following:

- Init failed. Time Service exiting - Initialization error, but the time server exits.
- Synchronizing time of day clock - Usually logged during temporary operational issues when the clock goes out of synchronization. For example, when a time update packet is missed due to fabric reconfiguration or role change of the principal or primary fabric configuration server (FCS) switch. If the message does not recur, it can be ignored.
- Validating time update - Usually logged during temporary operational issues when a time update packet cannot be validated in a secure fabric. For example, during fabric reconfiguration or role change of the primary FCS switch. If the message does not recur, it can be ignored.

Recommended Action

Execute the `secPolicyShow` command to verify that the FCS policy is consistent across the fabric.

TS-1007**Message**

<message>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that a switch is trying to set the clock server, which is not the primary fabric configuration server (FCS) across the fabric. A consistent FCS policy must be implemented across the fabric.

Recommended Action

Execute the `secPolicyShow` command to verify that the FCS policy is consistent across the fabric.

TS-1008**Message**

<New clock server used> Clock Server used instead of <Old server configured>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the source of fabric time synchronization distributed from the principal or primary fabric configuration server (FCS) switch was changed to another configured clock server. This happens when the Network Time Protocol (NTP) query to the current active external clock server failed.

TS-1009

Message

Date changed by user from <Old system time> to <Updated system time by the user>.

Message Type

LOG | AUDIT

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates that the system date has been changed by the user.

TS-1010

Message

NTP Server Time Update from <Old system time> to <Updated system time received from NTP server>

Message Type

LOG | AUDIT

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates that the time is updated by the Network Time Protocol (NTP) server.

TS-1011

Message

<message>.

Message Type

LOG | AUDIT | FFDC

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates that the hardware clock update has failed.

Recommended Action

Collect supportsave and report to vendor.

TS-1012

Message

Timezone changed from <Old Timezone> to <New Timezone>

Message Type

LOG | AUDIT

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates that the system timezone is modified.

TS-1013

Message

NTP Clock Server List modified to <New NTP Server List> from <Old NTP Server List>.

Message Type

LOG | AUDIT

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates the fabric time synchronization "NTP Clock Server List" is modified

TS-1014**Message**

NTP Key Index List modified to <New NTP Key Index List> from <Old NTP Key Index List>.

Message Type

LOG | AUDIT

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates the symmetric authentication "NTP Key Index List" is modified

TS-1015**Message**

NTP Key with index <NTP Key Index> and key type <NTP Key Type> added.

Message Type

LOG | AUDIT

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates a symmetric authentication key is added

TS-1016**Message**

NTP Key with index <NTP Key> deleted.

Message Type

LOG | AUDIT

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates a symmetric authentication key is deleted

TS-1017

Message

NTP authentication <enabled/disabled>.

Message Type

LOG | AUDIT

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates NTP authentication is enabled/disabled

TS-1018

Message

NTP legacy mode <enabled/disabled>.

Message Type

LOG | AUDIT

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates NTP legacy mode is enabled/disabled

TS-1019**Message**

System clock update(<New time to be updated>) rejected, request exceeds RTA(<RTA estimated system time>) threshold.

Message Type

LOG | AUDIT

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates the time to be updated exceeds the RTA allowed threshold

Recommended Action

If this message is seen continuously, please verify the system clock and the clock sources across the fabric switches. If the date is off by more than +/- 7 days, please reach out to TAC for further assistance. It is normal to see this message one time during system initialization or HA events due to convergence.

TS-1020**Message**

NTP Clock Server List configuration failed for <NTP Server List>.

Message Type

LOG | AUDIT

Message Class

SECURITY

Message Severity

INFO

Probable Cause

Indicates that Network Time Protocol (NTP) clock server configuration failed.

Recommended Action

Verify that the NTP clock servers in the list are available and functional. If the NTP clock servers in the list are not available, choose another set of clock servers.

UCID Messages

UCID (Unified Configuration Infrastructure Daemon) module error messages.

UCID-1001

Message

roll back message failed

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates a failure in rollback.

Recommended Action

No action to be taken.

UCID-3001

Message

Enabled FCOE provisioning on port <port_name>

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the port is being Fibre Channel over Ethernet(FCoE) provisioned.

UCID-3002

Message

Removed FCOE provisioning on port <port_name>

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the port is being Fibre Channel over Ethernet(FCoE) provisioned.

UCID-3003

Message

<enodes> enodes created

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the enodes have been successfully configured.

UCID-3004

Message

FCMAP is updated to <fcmap> for fabric-map <fabricmap>

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the fcmmap have been successfully updated.

UCID-3005**Message**

FCoE VLAN is updated to <vlan> for fabric-map <fabricmap>

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the VLAN has been successfully updated.

UCID-3006**Message**

FCoE Priority is updated to <priority> for fabric-map <fabricmap>

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the priority has been successfully updated.

UCID-3007

Message

FCoE FKA Timeout is updated to <timeout>

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the timeout has been successfully updated.

UCID-3008

Message

FCoE FKA Interval is updated to <fka>

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the FKA interval has been successfully updated

UCID-3009

Message

CEE QoS priority group table updated for group number <port_name> with PFC <pfc>

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that Converged Enhanced Ethernet(CEE) QoS priority group table updated for group number.

UCID-3010**Message**

CEE QoS priority table updated to <pg_tbl_num_1> <pg_tbl_num_2> <pg_tbl_num_3> <pg_tbl_num_4> <pg_tbl_num_5> <pg_tbl_num_6> <pg_tbl_num_7>

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that Converged Enhanced Ethernet(CEE) QoS priority table is updated.

UCID-3011**Message**

CEE Qos enabled on port <port_name>

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that Converged Enhanced Ethernet(CEE) QoS is enabled for port.

UCID-3012**Message**

CEE Qos disabled on port <port_name>

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that Converged Enhanced Ethernet(CEE) QoS is disabled for port.

UCID-3013**Message**

CEE Qos updated to default configuration

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the Converged Enhanced Ethernet(CEE) Qos configuration is updated to default.

UCID-3014**Message**

LLDP global configuration are enabled on all ports

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that Link Layer Discovery Protocol(LLDP) global configuration is enabled on all ports.

UCID-3015**Message**

LLDP global configuration are disabled on all ports

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that Link Layer Discovery Protocol(LLDP) global configuration is disabled on all ports.

UCID-3016**Message**

LLDP parameter system name is configured to <sys_name>

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that Link Layer Discovery Protocol(LLDP) global configuration system name is being updated.

UCID-3017**Message**

LLDP parameter system description is configured to <sys_desc>

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that Link Layer Discovery Protocol(LLDP) global configuration system description is being updated.

UCID-3018**Message**

LLDP parameter transmit interval is configured to <tx_intvl>

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that Link Layer Discovery Protocol(LLDP) global configuration transmit interval is being updated.

UCID-3019**Message**

LLDP parameter timeout multiplier is configured to <mul>

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that Link Layer Discovery Protocol(LLDP) global configuration timeout multiplier is being updated.

UCID-3020**Message**

LLDP parameter ISCSI priority is configured to <prio>

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that Link Layer Discovery Protocol(LLDP) global configuration ISCSI priority is being updated.

UCID-3021**Message**

LLDP parameter descriptor name is configured to <desc>

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that Link Layer Discovery Protocol(LLDP) global configuration descriptor name is being updated.

UCID-3022**Message**

LLDP parameter <tlv_name> tlv is enabled

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that Link Layer Discovery Protocol(LLDP) global configuration tlv is being set.

UCID-3023**Message**

LLDP parameter <tlv_name> tlv is disabled

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that Link Layer Discovery Protocol(LLDP) global configuration tlv is being disabled.

UCID-3025**Message**

LLDP profile <profile_name> created

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that Link Layer Discovery Protocol(LLDP) profile is being created.

UCID-3026**Message**

LLDP profile <profile_name> deleted

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that Link Layer Discovery Protocol(LLDP) profile is being deleted.

UCID-3027**Message**

LLDP profile <profile_name> parameter descriptor updated to <desc_name>

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that Link Layer Discovery Protocol(LLDP) profile descriptor is being updated.

UCID-3028**Message**

LLDP profile <profile_name> parameter transmit interval updated to <tx_intvl>

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that Link Layer Discovery Protocol(LLDP) profile transmit interval is being updated.

UCID-3029**Message**

LLDP profile <profile_name> parameter timeout multiplier updated to <mul>

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that Link Layer Discovery Protocol(LLDP) profile timeout multiplier is being updated.

UCID-3030**Message**

LLDP profile <profile_name> parameter <tlv_name> tlv is enabled

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that Link Layer Discovery Protocol(LLDP) profile tlv is being set.

UCID-3031

Message

LLDP profile <profile_name> parameter <tlv_name> tlv is disabled

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that Link Layer Discovery Protocol(LLDP) profile tlv is being disabled.

UCID-3032

Message

LLDP has been enabled on port <port_name>

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that Link Layer Discovery Protocol(LLDP) has been enabled on port.

UCID-3033**Message**

LLDP has been disabled on port <port_name>

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that Link Layer Discovery Protocol(LLDP) has been disabled on port.

UCID-3034**Message**

LLDP parameter dcbx version is updated to <cee_version> on port <port_name>

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that Link Layer Discovery Protocol(LLDP) parameter dcbx version is updated on port.

UCID-3035**Message**

LLDP profile <profile_name> is added to port <port_name>

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that Link Layer Discovery Protocol(LLDP) profile is added to port.

UCID-3036**Message**

LLDP profile is removed from port <port_name>

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that Link Layer Discovery Protocol(LLDP) profile is removed from port.

UCID-3037**Message**

Cleared LLDP neighbor devices for port <port_name>

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Cleared Link Layer Discovery Protocol(LLDP) neighbors for port.

UCID-3038**Message**

Cleared LLDP stats for port <port_name>

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Cleared Link Layer Discovery Protocol(LLDP) stats for port.

UCID-3039**Message**

Cleared LLDP neighbor devices for all ports

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Cleared Link Layer Discovery Protocol(LLDP) neighbors for port.

UCID-3040**Message**

Cleared LLDP stats for all ports

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Cleared Link Layer Discovery Protocol(LLDP) stats for port.

UCID-3041

Message

PortChannel <po> is created with type <type>, speed <speed>, key <key> and port member <port_member>

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

portchannel is created.

UCID-3042

Message

PortChannel <po> is deleted

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

portchannel is deleted.

UCID-3043**Message**

PortChannel <po> is enabled

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

portchannel is enabled.

UCID-3044**Message**

PortChannel <po> is disabled

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

portchannel is disabled.

UCID-3045**Message**

Port <port_name> is added to portchannel <po>

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

port member is added to portchannel.

UCID-3046**Message**

Port <port_name> is removed from portchannel <po>

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

port member is removed from portchannel.

UCID-3047**Message**

LACP system priority is updated to <priority>

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

set Link Aggregation Control Protocol(LACP) sytem priority.

UCID-3048**Message**

PortChannel <po> is updated with speed <speed>

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

portchannel Speed is updated.

UCID-3049**Message**

PortChannel <po> is updated with auto neg <auto_neg>

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

portchannel auto neg is updated.

UCID-3050**Message**

Member port <po> of PortChannel <po_num> is set to priority <priority>

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

member port priority is updated.

UCID-3051

Message

Member port <po> of PortChannel <po_num> is set with timeout <timeout>

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Member port timeout is updated.

UCID-3052

Message

Cleared FCOE stats on port <port_name>

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

cleared Fibre Channel over Ethernet(FCoE) stats for individual ports.

UCID-3053**Message**

Cleared FCOE stats on all ports

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

cleared Fibre Channel over Ethernet(FCoE) stats for all ports.

UCID-3054**Message**

FCoE Fabric-map <fabricmap> is created with fcmmap <fcmmap>, vlan <vlan> and priority <priority>

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the fabric-map have been successfully created.

UCID-3055**Message**

Fabric-map <fabricmap> is deleted

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the fabric-map have been successfully removed.

UCID-3056

Message

Cleared portchannel <lag_name> stats

Message Type

AUDIT

Message Class

CFG

Message Severity

INFO

Probable Cause

cleared portchannel stats for all ports.

UCST Messages

Unicast routing table module error messages.

UCST-1003

Message

Duplicate Path to Domain <domain ID>, Output Port = <port number>, PDB pointer = 0x<value>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that duplicate paths were reported to the specified domain from the specified output port. The *PDB pointer* value displayed in the message is the address of the path database and provides debugging information.

UCST-1007**Message**

Inconsistent route detected: Port = <port number>, should be <port number>.

Message Type

FFDC | LOG

Message Severity

CRITICAL

Probable Cause

Indicates that the switch detected an inconsistency in the routing database between the routing protocol and the hardware configuration. The first port number displayed is what the hardware has configured and the second port number displayed is what the protocol is using.

Recommended Action

Run the `switchDisable` command and then the `switchEnable` command to reset the routing database. Run the `uRouteShow` command to display the new routing tables.

UCST-1020**Message**

Static route (input-area: <port number>, domain: <domain ID> output-area: <port number>) has been ignored due to platform limitation.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the configured static route cannot be applied to the routing database because of a platform limitation.

UCST-1021**Message**

In-order delivery option has been enabled.

Message Type

AUDIT | LOG

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that in-order delivery (IOD) option has been enabled on the switch. This option guarantees in-order delivery of frames during fabric topology changes.

UCST-1022

Message

In-order delivery option has been disabled.

Message Type

AUDIT | LOG

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that in-order delivery (IOD) option has been disabled on the switch. This may cause out-of-order delivery of frames during fabric topology changes.

UCST-1023

Message

Dynamic Load Sharing option has been enabled

Message Type

AUDIT | LOG

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that Dynamic Load Sharing (DLS) option has been enabled on the switch. This will move existing routes to a new redundant path when this path becomes available.

UCST-1024**Message**

Dynamic Load Sharing option has been disabled.

Message Type

AUDIT | LOG

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that Dynamic Load Sharing (DLS) option has been disabled on the switch.

UCST-1026**Message**

LossLess-DLS option has been enabled.

Message Type

AUDIT | LOG

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the NoFrameDrop option has been enabled. This will help minimize frame loss during fabric topology changes.

UCST-1027

Message

LossLess-DLS option has been disabled.

Message Type

AUDIT | LOG

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the NoFrameDrop option has been disabled. This may cause higher frame loss during fabric topology changes.

UCST-1028

Message

E_Port Balance Priority option has been enabled by <functionName>.

Message Type

AUDIT | LOG

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that priority is given to make sure that E_Port bandwidth demand is balanced.

UCST-1029

Message

E_Port Balance Priority option has been disabled by <functionName>.

Message Type

AUDIT | LOG

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that priority is no longer given to balanced E_Port bandwidth demand when balancing routes.

UCST-1030

Message

Two-hop lossless option has been enabled.

Message Type

AUDIT | LOG

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the two-hop lossless capability has been enabled on the switch.

UCST-1031

Message

Two-hop lossless option has been disabled.

Message Type

AUDIT | LOG

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that the two-hop lossless capabilities have been disabled on the switch.

UCST-1032

Message

Route rebalance <printf>

Message Type

AUDIT | LOG

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that E_Port load rebalancing on this logical switch succeeded or failed

UCST-1033

Message

Route rebalance all <printf>

Message Type

AUDIT | LOG

Message Class

CFG

Message Severity

INFO

Probable Cause

Indicates that E_Port load rebalancing on all logical switches succeeded or failed

UFCS Messages

UFCS (Universal Fabric Configuration Service) module error messages.

UFCS-1001

Message

Test UFCS RAS Domain ID (<DomainId>).

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the Domain is valid.

Recommended Action

If the message persists, execute the `supportSave` command and contact your switch service provider.

UFCS-1002**Message**

UFCS Merge Conflict - clientId <Client Id> (<Client Id String>), cfgType <Configuration Type>, tagId 0x<Tag Id>, opFlag <Op Flag>, domain <Source Domain>, reason (<Failure Reason Code> - <Failure Reason Description>).

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that a Universal Fabric Configuration Service (UFCS) merge conflict occurred for the specified clientId and cfgType.

Recommended Action

Users should attempt to find the specified mismatched configuration and take corrective action to try and fix the conflict. If there does not appear to be a configuration conflict or the user is not able to locate the configuration specified, users can execute the `supportSave` command on both this domain and the remote domain specified by the domain field and contact your switch service provider.

UFCS-1003**Message**

Failed to allocate memory: (<function name>).

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates a failure to allocate memory.

Recommended Action

If the message persists, execute the `supportSave` command and contact your switch service provider.

UFCS-1004**Message**

UFCS Stuck Merge - clientId <Client Id> (<Client Id String>), cfgType <Configuration Type>, tagId 0x<Tag Id>, opFlag <Op Flag>, domain <Source Domain>.

Message Type

LOG | FFDC

Message Severity

WARNING

Probable Cause

Indicates that a merge in progress with a particular domain has been stuck for the max allowable duration.

Recommended Action

If the message persists, execute the `supportSave` command and contact your switch service provider.

UFCS-1005**Message**

The UFCS message queue has reached <the UFCS message queue usage high/low threshold limit> percent of its maximum limit.

Message Type

LOG | FFDC

Message Severity

WARNING

Probable Cause

Indicates that UFCS is receiving events faster than it can process them and the message queue is nearing its maximum limit.

Recommended Action

Execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

UFCS-2004**Message**

UFCS Commit stage Failed - clientId <Client Id> (<Client Id String>), cfgType <Configuration Type>, tagId 0x<Tag Id>, opFlag <Op Flag>, dom <Failure Domain>, client-rsn <Client Failure Reason Code>, UFCS-rsn (<UFCS Failure Reason Code> - <UFCS Failure Reason Code Description>).

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the Universal Fabric Configuration Service (UFCS) commit stage has failed.

Recommended Action

If the message persists, execute the `supportSave` command on both this domain and the remote domain specified by the domain field and contact your switch service provider.

UFCS-2005**Message**

UFCS Cancel stage Failed - clientId <Client Id> (<Client Id String>), cfgType <Configuration Type>, tagId 0x<Tag Id>, opFlag <Op Flag>, dom <Failure Domain>, client-rsn <Client Failure Reason Code>, UFCS-rsn (<UFCS Failure Reason Code> - <UFCS Failure Reason Code Description>).

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the Universal Fabric Configuration Service (UFCS) cancel stage has failed.

Recommended Action

If the message persists, execute the `supportSave` command on both this domain and the remote domain specified by the domain field and contact your switch service provider.

UFCS-2006

Message

UFCS Transaction Hung - clientId <Client Id> (<Client Id String>), cfgType <Configuration Type>, tagId 0x<Tag Id>, opFlag <Op Flag>, trans state <Trans State>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the update cannot be completed for an unknown reason.

Recommended Action

If the message persists, execute the `supportSave` command and contact your switch service provider.

UFCS-2007

Message

UFCS Lock stage Failed - clientId <Client Id> (<Client Id String>), cfgType <Configuration Type>, tagId 0x<Tag Id>, opFlag <Op Flag>, dom <Failure Domain>, client-rsn <Client Failure Reason Code>, UFCS-rsn (<UFCS Failure Reason Code> - <UFCS Failure Reason Code Description>).

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the Universal Fabric Configuration Service (UFCS) lock stage has failed.

Recommended Action

If the message persists, execute the `supportSave` command on both this domain and the remote domain specified by the domain field and contact your switch service provider.

UFCS-2008

Message

UFCS Timeout - clientId <Client Id> (<Client Id String>), cfgType <Configuration Type>, tagId 0x<Tag Id>, opFlag <Op Flag>, srcDom <Transaction Source Domain>, st <Transaction State at time of timeout>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the Universal Fabric Configuration Service (UFCS) transaction experienced a timeout condition.

Recommended Action

If the message persists, execute the `supportSave` command on both this domain and the remote domain specified by the domain field and contact your switch service provider.

UFCS-2009

Message

UFCS Lock stage Failed - clientId <Client Id> (<Client Id String>), cfgType <Configuration Type>, tagId 0x<Tag Id>, opFlag <Op Flag>, dom <Failure Domain>, client-rsn <Client Failure Reason Code>, UFCS-rsn (<UFCS Failure Reason Code> - <UFCS Failure Reason Code Description>).

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the Universal Fabric Configuration Service (UFCS) lock stage has failed.

Recommended Action

If the message persists, execute the `supportSave` command on both this domain and the remote domain specified by the domain field and contact your switch service provider.

UPTH Messages

UPTH module error messages.

UPTH-1001

Message

No minimum cost path in candidate list.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the switch is unreachable because no minimum cost path (MPATH) exists in the candidate list (domain ID list).

Recommended Action

No action is required. This error will end the current shortest path first (SPF) computation.

UPTH-1002**Message**

Domain <domain ID> is unreachable because the enabled TI zone is not compatible with the fabric configuration.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the specified switch is unreachable because the traffic isolation (TI) zone and the fabric configuration are incompatible.

Recommended Action

Clear all TI zones and then create a valid TI zone for your fabric configuration. Refer to the *Fabric OS Administrator's Guide* for more information on TI zoning.

USL Messages

USL error messages.

USL-1001**Message**

Interface <InterfaceName> is online.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the specified interface has come online after the protocol dependencies are resolved.

USL-1002**Message**

Interface <InterfaceName> is protocol down.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the specified interface has gone offline because one of the protocol dependencies is unresolved.

Recommended Action

Check for the reason codes using the `show interface` command and resolve the protocol dependencies.

The following are the possible reason codes:

- Admin down
- Link protocol down
- DOT1x authenticating
- Minimum member links not UP (applicable only for port-channel interfaces)
- DOT1x authentication failed
- BRCD remote link negotiation failed/LLDP disabled
- LAG negotiating/failed
- LAG admin state is down
- UNKNOWN

USL-1003**Message**

Interface <InterfaceName> is link down.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the specified interface has gone offline because the link is down.

Recommended Action

Check whether the connectivity between the peer ports is proper, and the remote link is up using the `show interface` command.

USL-1004

Message

Interface <InterfaceName> is created.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the specified logical interface has been created.

USL-1005

Message

The FCoE VLAN: <VlanName> is in use. Therefore, cannot disable the FCoE VLAN.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the specified Fibre Channel over Ethernet (FCoE) VLAN is used in the FCoE daemon (fcoed) and therefore cannot be disabled.

Recommended Action

Remove all the FCoE sessions from the FCoE VLAN member ports and then disable the FCoE VLAN.

USL-1006

Message

FCoE on VLAN: <VlanName> has been disabled successfully.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that FCoE has been disabled on the specified VLAN.

USL-1007

Message

Chassis is <status>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the chassis has been enabled or disabled.

USL-1008

Message

Blade (<slot number>) is <status>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the specified blade has been enabled or disabled.

USL-1009

Message

Interface <InterfaceName> is deleted.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the specified logical interface has been deleted.

USL-1010

Message

InterfaceMode changed from <Mode_old> to <Mode_new> for interface <InterfaceName>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the interface mode has been changed.

USL-1011

Message

OperationalEndpointMode changed from <Mode_old> to <Mode_new> for interface <InterfaceName>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the interface operational endpoint mode has been changed.

USL-1012

Message

VLAN classifier group <group_id> is created.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the specified VLAN classifier group has been created.

USL-1013

Message

VLAN classifier group <group_id> is deleted.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the specified VLAN classifier group has been deleted.

USL-1014

Message

VLAN classifier rule <rule_id> is created.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the specified VLAN classifier rule has been created.

USL-1015

Message

VLAN classifier rule <rule_id> is deleted.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the specified VLAN classifier rule has been deleted.

USL-1016

Message

VLAN classifier rule <rule_id> is <action> on VLAN classifier group <group_id>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the specified VLAN classifier group has been modified.

USL-1017

Message

Interface <InterfaceName> is <action> on interface <Logical_InterfaceName>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the logical interface member list has been changed.

USL-1018

Message

<count> VLANs <except> will be allowed on interface <Logical_InterfaceName>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the VLAN membership has been changed for the specified interface.

USL-1019

Message

Interface <InterfaceName> is administratively up.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the administrative status of the specified interface has changed to up.

USL-1020

Message

Interface <InterfaceName> is administratively down.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the administrative status of the specified interface has changed to down.

VS Messages

VS module messages.

VS-1001

Message

No virtual PWWN assignment for the device <Login device PWWN>, port <Switch port> or (AG <AG NWWN> port <AG port>).

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the device with the virtual Port World Wide Name (PWWN) feature enabled tried to log in but there is no mapping for the device, port, or Access Gateway (AG) port.

Recommended Action

Execute the `fapwwn` command to map the device, port, or AG port. You can ignore this message if the virtual PWWN is not required.

VS-1002

Message

The Virtual PWWN assignment for the device <Login device PWWN>, port <Switch port> (AG <AG NWWN> port <AG port>) is timed out.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the virtual Port World Wide Name (PWWN) association has timed out.

VS-1003

Message

Could not find Virtual PWWN config file for the switch.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the configuration file is corrupted or accidentally removed.

Recommended Action

Restart the switch and download the configuration using the `configDownload` command.

VS-1004

Message

Could not find Virtual PWWN config file for the switch.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the virtual Port World Wide Name (PWWN) feature has been enabled for the first time on the switch or the configuration file was corrupted or accidentally removed.

Recommended Action

Creating a new default configuration file. Execute the `configDownload` command to download any of your earlier configurations for the virtual PWWN feature.

VS-1005

Message

Virtual PWWN config version mismatch detected.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the virtual Port World Wide Name (PWWN) configuration present on the switch is not of the same Fabric OS version.

Recommended Action

Converting the virtual PWWN configuration to the current Fabric OS version. No action is required.

VS-1006**Message**

Virtualization services failed to initialize due to lack of enough memory.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the system has run out of memory.

VS-1007**Message**

FSS Registration failed for virtualization services.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates failure in the virtualization service daemon (vsd) startup because vsd has failed to register with Fabric OS State Synchronization (FSS).

VS-1008**Message**

Virtualization services failed to create timer.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates failure in the virtualization service daemon (vsd) startup because vsd has failed to create a timer.

WEBD Messages

WEBD module messages indicate problems with the Web Tools module.

WEBD-1001

Message

Missing or Invalid Certificate file -- HTTPS is configured but could not be started.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates the Secure Sockets Layer (SSL) certificate file is either invalid or absent.

Recommended Action

Install a valid certificate file.

WEBD-1002

Message

Missing or Invalid Key file -- HTTPS is configured but could not be started.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates the Secure Sockets Layer (SSL) key file is either invalid or absent.

Recommended Action

Install a valid key file.

WEBD-1004**Message**

HTTP server and weblinker process will be restarted due to configuration change.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates the Hypertext Transfer Protocol (HTTP) server configuration has changed.

WEBD-1005**Message**

HTTP server and weblinker process will be restarted for logfile truncation.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates the size of the Hypertext Transfer Protocol (HTTP) log file exceeded the maximum limit.

WEBD-1006**Message**

HTTP server and weblinker restarted due to logfile truncation.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates the size of the Hypertext Transfer Protocol (HTTP) log file exceeded the maximum limit.

WEBD-1007**Message**

HTTP server and weblinker process will be restarted due to change of IP Address.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates the IP address of the switch changed and the Hypertext Transfer Protocol (HTTP) server is restarted.

WEBD-1008**Message**

HTTP server and weblinker process cannot be started.

Message Type

LOG | FFDC

Message Severity

WARNING

Probable Cause

Indicates a rare error condition in which the built-in recovery process has failed to restore Hypertext Transfer Protocol (HTTP) services. The problem often results from invalid configuration of Secure Sockets Layer (SSL) certificates, but there can be more than one reason for such a failure.

Recommended Action

Verify the certification file; there may be a mismatch involved.

WEBD-1009**Message**

HTTPS is disabled due to invalid certificate.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates a condition where HTTPS cannot be enabled since certificate file is invalid and HTTP is enabled

XTUN Messages

XTUN module error messages.

XTUN-1000

Message

FTNL Tunnel <VE Port (Tunnel) Number> Missed Data frame:I/T/L:<FC Initiator ID>/<FC Target ID>/<FCP Logical Unit Number>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates a missed frame with one or more Fibre Channel Protocol (FCP) data information units during a SCSI write or read operation.

Recommended Action

If there was an unexpected job failure associated with this event, contact your vendor's customer support for assistance.

XTUN-1001

Message

FTNL Tunnel <VE Port (Tunnel) Number> Memory allocation failed tracker <Number that represents the calling source module>/<Line number in that source file>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates a memory allocation failure.

Recommended Action

Contact your vendor's customer support for assistance.

XTUN-1002**Message**

FTNL Tunnel <VE Port (Tunnel) Number> Exchange timeout:I/T/L:<FC Initiator ID>/<FC Target ID>/<FCP Logical Unit Number>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the Fibre Channel Protocol (FCP) exchange has timed out.

Recommended Action

If there was an unexpected job failure associated with this event, contact your vendor's customer support for assistance.

XTUN-1003**Message**

FTNL Tunnel <VE Port (Tunnel) Number> Message Transmission failed:I/T/L/E:<FC Initiator ID>/<FC Target ID>/<FCP Logical Unit Number>/<Error return value>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates a message transmission failure.

Recommended Action

If there was an unexpected job failure associated with this event, contact your vendor's customer support for assistance.

XTUN-1004

Message

FTNL Tunnel <VE Port (Tunnel) Number> Exchange aborted:I/T/L:<FC Initiator ID>/<FC Target ID>/<FCP Logical Unit Number>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the Fibre Channel Protocol (FCP) exchange has been aborted by the initiator.

Recommended Action

If there was an unexpected job failure associated with this event, contact your vendor's customer support for assistance.

XTUN-1005

Message

FCP emulation for Tunnel/Initiator/Target/LUN:<VE Port (Tunnel) Number>/<FC Initiator ID>/<FC Target ID>/<FCP Logical Unit Number> may not be optimal.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the Fibre Channel Protocol (FCP) emulation is in FastWrite mode and could also be in Tape Pipelining mode.

Recommended Action

For disk devices, no action is required. For tape devices, device rediscovery is required.

XTUN-1006

Message

FCIP FC frame drop due to transmit timeout on slot=<FX8-24/SX6 Slot Number (0 for 7800 and 7840)> DP=<FX8-24/SX6/7840 DP Number (or 0 if 7800)> BLS=<Blaster Image Number (0 or 1)> DR=<FC Descriptor Ring Number> Frames Dropped=<Number of FC frames that were dropped>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that a Fibre Channel (FC) Send frame timeout occurred and the frames were dropped from the SW queue.

Recommended Action

This error indicates that there is a slow draining device or a hung Blaster TX Descriptor Ring.

XTUN-1007**Message**

FCIP FC frame drop due to truncated receive on slot=<FX8-24/SX6 Slot Number (0 for 7800 and 7840)> DP=<FX8-24/SX6/7840 DP Number (or 0 if 7800)> BLS=<Blaster Image Number (0 or 1)> DR=<FC Descriptor Ring Number> Frames Dropped=<Number of FC frames that were dropped>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that a Fibre Channel (FC) Received frame event was posted, but the frame was dropped due to an invalid receive length. This error occurs only on faulty hardware.

Recommended Action

Contact your vendor's customer support for assistance.

XTUN-1008**Message**

FCIP Control block memory usage slot=<FX8-24/SX6 Slot number (0 for 7800 or 7840)> DP=<FX8-24/SX6/7840 DP number (or 0 if 7800)> Allocated=<The total allocated bytes from the pool> Free=<The total free bytes remaining in the pool> Total=<The total size of the pool>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the control block memory pool has crossed the usage threshold. This message is generated when a significant amount of control block memory has been allocated from the free pool. This memory is limited and you should monitor for events that indicate that greater than 80 percent of the pool has been allocated.

Recommended Action

Contact your vendor's customer support for assistance.

XTUN-1009**Message**

FCIP OSTP <Number of FCP write commands that were purged> Write blocks purged due to PLOGI slot=<FX8-24/SX6 Slot number (0 for 7800 or 7840)> DP=<FX8-24/SX6/7840 DP number (or 0 if 7800)> SFID=<SFID of the initiator> DFID=<DFID of the tape device> SID/DID/Lun=0x<SID of the initiator>/<DID of the tape device>/<The tape device LUN number>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that more than one outstanding write command that were purged due to the receipt of a new PLOGI sequence. This can indicate missing blocks on the currently mounted tape. If the tape job resumed after this error, you must confirm the integrity of the data on the tape.

Recommended Action

Contact your vendor's customer support for assistance.

XTUN-1010**Message**

FCIP FC RCV frame drop due to <Reason> on slot=<Slot Number (0 for 7840)> DP=<DP Number> FPGA=<FPGA Image Number (0 or 1)> VC=<Virtual Circuit (VC) number> Frames Dropped=<Number of FC frames that were dropped>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that a Fibre Channel (FC) received frame event was posted, but the frame was dropped due to a receive error. This error is likely due to upstream crc errors.

Recommended Action

Contact your vendor's customer support for assistance.

XTUN-1996**Message**

FTRACE buffer <FTRACE Trace Buffer Number> on slot <FX8-24/SX6 Slot Number (0 for 7800 and 7840)> DP <FX8-24/SX6/7840 DP Number (or 0 if 7800)> has been cleared.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that a CLI command or `supportSave` operation freed the trace buffer back into the FTRACE free pool.

XTUN-1997**Message**

FTRACE buffer <FTRACE Trace Buffer Number> on slot <FX8-24/SX6 Slot number (0 for 7800 or 7840)> dp <FX8-24/SX6/7840 DP number (or 0 if 7800)> has been triggered.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that a programmed trigger event has been detected.

Recommended Action

If there was an unexpected job failure associated with this event, contact your vendor's customer support for assistance.

XTUN-2012

Message

IKE: Session DP<DP-ID>.<IKE Session ID> <Authentication Method> Authentication failure.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the specified Internet Key Exchange (IKE) session authentication has failed.

Recommended Action

Manual recovery of the IKE session is required. See FCIP Admin Guide for recovery steps, or contact your vendor's customer support for assistance.

XTUN-2013

Message

IKE: Session DP<DP-ID>.<IKE Session ID> <IKE Transform Parameter> mismatch detected: expected <Configured IKE Transform Value>, got <Received IKE Transform Value>

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the specified Internet Key Exchange (IKE) session transform parameter cannot be negotiated correctly.

Recommended Action

The configuration must be corrected to match on both sides of the IKE connection, then manual recovery of the IKE session is required. See FCIP Admin Guide for recovery steps, or contact your vendor's customer support for assistance.

XTUN-2014

Message

IKE: Session DP<DP-ID>.<IKE Session ID> Responder rejected INIT request

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the specified Internet Key Exchange (IKE) session was rejected by the connection responder.

Recommended Action

See the peer side logs for further information on the failure reason. Manual recovery of the IKE session is required. See FCIP Admin Guide for recovery steps, or contact your vendor's customer support for assistance.

XTUN-2015**Message**

IKE: Session DP<DP-ID>.<IKE Session ID> unable to program <FPGA select type> value

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates the specified FPGA memory segment failed a write/read verification.

Recommended Action

The affected IKE session will be automatically deleted and restarted. If the issue persists, contact your vendor's customer support for assistance.

XTUN-3000**Message**

WAN Tool session <WAN Tool Session ID> ENABLED.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the specified WAN Tool session has been administratively enabled.

XTUN-3001**Message**

WAN Tool session <WAN Tool Session ID> DISABLED.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the specified WAN Tool session has been administratively disabled.

XTUN-3002**Message**

WAN Tool session <WAN Tool Session ID> STARTED.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the specified WAN Tool session traffic has been administratively started.

XTUN-3003**Message**

WAN Tool session <WAN Tool Session ID> STOP.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the specified WAN Tool session traffic has been administratively stopped.

XTUN-3004**Message**

WAN Tool session <WAN Tool Session ID> SLA Negotiated Drop: <WAN Tool SLA Drop percentage>, Runtime: <WAN Tool SLA Runtime time>, Timeout: <WAN Tool SLA Timeout time>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the specified WAN Tool session has negotiated its Service Level Agreement (SLA) configuration.

XTUN-3005**Message**

WAN Tool session <WAN Tool Session ID> SLA Failed to negotiate Reason <WAN Tool Failure Reason>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the specified WAN Tool session has failed to negotiate its Service Level Agreement (SLA) configuration for the specified reason.

Recommended Action

Check peer SLA configuration and network connectivity.

XTUN-3006**Message**

WAN Tool session <WAN Tool Session ID> SLA Failed to meet SLA requirements Reason <WAN Tool Failure Reason>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the specified WAN Tool session has failed to meet the Service Level Agreement (SLA) requirements for the specified reason.

XTUN-3007**Message**

WAN Tool session <WAN Tool Session ID> SLA requirements meet.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the specified WAN Tool session has successfully met the requirements for the configured Service Level Agreement (SLA).

XTUN-3008**Message**

WAN Tool session <WAN Tool Session ID> has completed.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the specified WAN Tool session has successfully completed running traffic.

XTUN-3009

Message

WAN Tool session <WAN Tool Session ID> STOP, Reason: <WAN Tool Stop Reason> request.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the specified WAN Tool session traffic has been administratively stopped for the specified reason.

XTUN-3010

Message

WAN Tool session <WAN Tool Session ID> <WAN Tool Negotiation Failure Type> negotiation failed, local/remote: <WAN Tool Configuration Values>. <WAN Tool Min/Max/Error Value>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the configuration value could not be negotiated.

XTUN-3100

Message

TCP:Slot=<Slot Number(0 for 7840)> DP=<DP ID>:Reaching maximum TCP connection limit:<Active Connection Count> of <Maximum Supported TCP Connections>.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the maximum supported TCP connection limit is reaching.

Recommended Action

Make sure not to initiate new replications.

XTUN-3101**Message**

TCP:Slot=<Slot Number(0 for 7840)> DP=<DP ID>:New TCP connections dropped:<Total number of local/remote connection open failures>, Max supported TCP connections:<Maximum Supported TCP Connections> reached.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the new TCP connection has failed.

Recommended Action

Make sure not to initiate new replications.

XTUN-3102**Message**

TCP:Slot=<Slot Number(0 for 7840)> DP=<DP ID>:New TCP connection dropped, NULL VLAN ID in SYN packet:<Source IP address/port of dropped connection>-<Destination IP address/port of dropped connection>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the new TCP connection has failed.

Recommended Action

Check host configuration for valid VLAN ID.

ZONE Messages

Zone module error messages.

ZONE-1003

Message

zone(<current zone>) contains (<domain id>, <port number>) which does not exist.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the port zone member that is targeted for the local switch contains a nonexistent port. The specified port number in the effective zoning configuration (displayed in the error message) is out of range.

Recommended Action

Edit the zone database and change the port number to a viable value in the effective configuration.

ZONE-1004

Message

Base PID: 0x<Base PID>, Port Index: <Port Index>, Port: <Slot/Port>: enforcement changed to Session-based HARD Zoning.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the zoning enforcement has changed to session-based hard zoning due to one of the following conditions:

- The zone has a mix of WWN and domain,index (D,I) members.
- The Source Identifier (S_ID) list of the hardware-enforced zoning exceeded the S_ID limit.

ZONE-1007

Message

ioctl (<function>) in (<error message>) at port (<port number>) returns code (<error string>) and reason string (<reason string>).

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that frame filter logic reported a failure during the specified I/O Control (IOCTL) call. This is usually a programming error when adding CAM entries before the filter setup.

Recommended Action

Avoid this problem in the following ways:

- Avoid having too many hosts zoned with a set of target devices at a single port.
- Avoid having too many zones directed at a single port group on the switch.

ZONE-1010

Message

Duplicate entries detected in zone '<zone name>' for member '<duplicate member>'

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that there are duplicate entries in the specified zone object. This message occurs only when enabling a zone configuration.

Recommended Action

Check the members of the zone using the `cfgShow` command. Delete the duplicate member using the `zoneRemove` command.

ZONE-1015

Message

Not owner of the current transaction <transaction ID>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that a zoning change operation is not allowed because the zoning transaction is opened by another task.
Indicates concurrent modification of the zone database by multiple administrators.

Recommended Action

Wait until the previous transaction is completed. Verify that only one administrator is working with the zone database at a time.

ZONE-1017

Message

FA Zone(<zone name>) contains incorrect number of Initiator and Target devices.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the fabric assist (FA) zoning configuration has more than one initiator. This is because of incorrect entries in the FA zoning configuration.

Recommended Action

Edit the zone database to make sure that only one initiator is set for each FA zone configuration.

ZONE-1019

Message

Transaction Commit failed. Reason code <reason code> (<Application reason>) - \"<reason string>\".

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that reliable commit service (RCS) had a transmit error. RCS is a protocol used to transmit changes to the configuration database within a fabric.

Recommended Action

Often this message indicates a transitory problem. Wait a few minutes and retry the command.

Make sure your changes to the zone database are not overwriting the work of another administrator.

Execute the `cfgTransShow` command to determine if there is any outstanding transaction running on the local switches.

If the problem persists, execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

ZONE-1022

Message

The effective configuration has changed to <Effective configuration name>. <AD Id>

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the effective zone configuration has changed to the specified zone name.

Recommended Action

Verify that the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

ZONE-1023

Message

Switch connected to port (<port number>) is busy. Retrying zone merge.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the switch is retrying the merge operation. This usually occurs if the switch on the other side of the port is busy.

Recommended Action

If the problem persists, execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

ZONE-1024

Message

<Information message>.

Message Type

AUDIT | LOG

Message Class

ZONE

Message Severity

INFO

Probable Cause

Indicates that the `cfgSave` command has completed successfully.

ZONE-1026

Message

port <port number> Out of CAM entries.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the total number of entries of S_ID CAM is above the limit while creating or adding a zone group. The maximum number of CAM entries allowed depends on the application-specific integrated circuit (ASIC).

Recommended Action

If hardware zoning enforcement is preferred, edit the zoning database to have zoned port IDs (PIDs) for that port.

ZONE-1027**Message**

Zoning transaction aborted <error reason>. <AD Id>

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates the zoning transaction was aborted because of a variety of potential errors. The *error reason* variable can be one of the following conditions:

- Zone Merge Received: The fabric is in the process of merging two zone databases.
- Zone Config update Received: The fabric is in the process of updating the zone database.
- Bad Zone Config: The new configuration is not viable.
- Zoning Operation failed: A zoning operation failed.
- Shell exited: The command shell has exited.
- Unknown: An error was received for an unknown reason.
- User Command: A user aborted the current zoning transaction.
- Switch Shutting Down: The switch is currently shutting down.

Most of these error conditions are transitory.

Recommended Action

Try again after some time. Verify that only one administrator is modifying with the zone database at a time.

ZONE-1028**Message**

Commit zone DB size is larger than the supported limit of the fabric - <zone db size> greater than <max zone db size>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the zone database size is greater than the limit allowed by the fabric. The limit of the zone database size depends on the lowest level switch in the fabric. Older switches have less memory and force a smaller zone database for the entire fabric.

Recommended Action

Execute the `cfgSize` command to view the zone database size information. Edit the zone database to keep it within the allowable limit for the specific switches in your fabric.

ZONE-1029**Message**

Restoring zone cfg from flash failed [<return code>].

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the zone configuration restored from flash memory was faulty.

Recommended Action

If the problem persists, execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

ZONE-1034**Message**

A new zone database file is created.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that a new zone database file has been created.

ZONE-1036

Message

Unable to create <config file name>: error message <System Error Message>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the Fabric OS cannot create the zone configuration file. Typically, the zone configuration is too large for the memory available on the switch.

Recommended Action

Reduce the size of the zone database and retry the operation.

ZONE-1037

Message

Unable to examine <config file name>: error message <System Error Message>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the Fabric OS cannot examine the zone configuration file. Typically, the zone configuration is too large for the memory available on the switch.

Recommended Action

Reduce the size of the zone database and retry the operation.

ZONE-1038

Message

Unable to allocate memory for <config file name>: error message <System Error Message>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the Fabric OS cannot allocate enough memory for the zone configuration file. Typically, the zone configuration is too large for the memory available on the switch.

Recommended Action

Reduce the size of the zone database and retry the operation.

ZONE-1039**Message**

Unable to read contents of <config file name>: error message <System Error Message>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the Fabric OS cannot read the zone configuration file. Typically, the zone configuration is too large for the memory available on the switch.

Recommended Action

Reduce the size of the zone database and retry the operation.

ZONE-1040**Message**

Merged zone database exceeds limit.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the Fabric OS cannot read the merged zone configuration file. Typically, the zone configuration is too large for the memory available on the switch.

Recommended Action

Reduce the size of the zone database and retry the operation.

ZONE-1041**Message**

Unstable link detected during merge at port (<Port number>).

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates a possible unstable link or faulty cable.

Recommended Action

Verify that the small form-factor pluggable (SFP) transceiver and the cable at the specified port are not faulty. Replace the SFP and the cable, if necessary.

ZONE-1042**Message**

The effective configuration has been disabled. <AD Id>

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the effective zone configuration has been disabled.

Recommended Action

Verify the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

ZONE-1043

Message

The Default Zone access mode is set to No Access.

Message Type

AUDIT | LOG

Message Class

ZONE

Message Severity

INFO

Probable Cause

Indicates that the Default Zone access mode is set to No Access.

Recommended Action

Verify the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

ZONE-1044

Message

The Default Zone access mode is set to All Access.

Message Type

AUDIT | LOG

Message Class

ZONE

Message Severity

INFO

Probable Cause

Indicates that the Default Zone access mode is set to All Access.

Recommended Action

Verify the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

ZONE-1045

Message

The Default Zone access mode is already set to No Access.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the Default Zone access mode is already set to No Access.

ZONE-1046

Message

The Default Zone access mode is already set to All Access.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the Default Zone access mode is already set to All Access.

ZONE-1048

Message

ZONE ACA is rejected on the standby.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the standby zoning component did not receive a syncdump command from the primary side.

Recommended Action

Synchronize the standby control processor (CP) using the `haSyncStart` command.

ZONE-1049**Message**

ZONE AD-DefZone conflict detected while system initialization.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that there is an Admin Domain (AD) Default Zone conflict.

Recommended Action

Verify that the default zoning mode for AD0 is set to No Access using the `defzone --show` command. If the default zoning mode is not set to No Access, execute the `defzone --noaccess` command and then execute the `cfgsave` command to commit the default zone mode change.

ZONE-1054**Message**

Default Zone All Access mode is set with Frame Redirection zones.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the Default Zone All Access mode will not grant all access behavior when the frame redirection zones are defined.

Recommended Action

Remove frame redirection zones or set the Default Zone access mode to No Access using the `defzone --noaccess` command.

ZONE-1059

Message

Unexpected TI routing behavior or a potentially unroutable TI configuration has been detected on local domain <Domain ID of the local Logical Switch where the error was detected>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the current fabric topology and TI zone configuration may result in an unroutable condition or an unexpected routing behavior.

Recommended Action

Execute the `zone --showTErrors` command on the specified switch to report the conflicting configuration details.

ZONE-1061

Message

Some trunk members are missing from failover disabled active TI zones.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that some members in the trunk group are not added to the failover-disabled TI zone. This will result in traffic disruption if the trunk member goes down.

Recommended Action

If any trunk member is included in the TI failover-disabled zone path, then always add all members from that group. Execute the `zone --showTitrunkerrors` command on the switch to find the missing trunk members in the TI zone.

ZONE-1062

Message

Defined and Effective zone configurations are inconsistent.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the defined and effective configurations are different.

Recommended Action

Execute the `cfgEnable` command to make both the configurations consistent.

ZONE-1064**Message**

Failed to update client capability to ESS (Exchange Switch Support) after maximum number of retries - return code <Failed return code>. Failing sync dump to standby CP.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that Exchange Switch Support (ESS) is unable to update its capability. Failed to send the sync dump to standby control processor (CP).

Recommended Action

Verify that HA synchronization has failed using the `haShow` command. If HA synchronization has failed, execute the `haSyncStart` command on active CP to resynchronize the HA state.

ZONE-1065**Message**

Zoning operation (<function>) at port index (<port index>) returns code (<error code>). Port reset required.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates hardware and software zoning enforcement is out of sync.

Recommended Action

Toggle the port using the `portDisable` and `portEnable` commands in order to recover zoning enforcement.

ZONE-1066**Message**

Zoning operation failed to complete on the local switch - code <Error Code>.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates an IPC error occurred between Name Server and Zone Server.

Recommended Action

The switch is in an inconsistent state and can be corrected only by a reboot or power cycle.

Upon reboot, if switch is unable to join the fabric due to a zone conflict, issue `cfgClear` command.

If there is an enabled-configuration, commit `cfgClear` operation by issuing `cfgDisable`.

If there is no enabled-configuration, commit `cfgClear` operation by issuing `cfgSave`.

ZONE-1067**Message**

QoS high zone with Flow ID 5 has been assigned to an alternate VC due to vTap and QoS high priority zoning compatibility mode.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that Virtual Tap (vTAP) and quality of service (QoS) high priority zoning compatibility mode is enabled and therefore the existing QoS H5 will be remapped to a lower virtual channel (VC).

ZONE-1068

Message

Admin Domains are not supported (Event:<Event Name>).

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that Admin Domains (ADs) are not supported.

ZONE-1069

Message

Admin Domains are not supported (Event:<Event Name>, AD<Admin Domain Number>).

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that Admin Domains (ADs) are not supported.

ZONE-1070

Message

Commit zone DB size exceeds the currently available limit in the chassis - <zone db size> greater than <max chassis zone db size>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the zone database size is greater than the limit allowed in the chassis.

Recommended Action

Execute the `cfgSize` command to view the zone database size information. Edit the zone database to keep it within the allowable chassis limit for the specific switches in your fabric.

ZONE-1071**Message**

Commit zone DB size is larger than the supported limit of domain <domain> - <zone db size> greater than <max zone db size>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the zone database size is greater than the limit allowed by the domain in the existing fabric. The limit of the zone database size depends on the lowest level switch in the fabric. Older switches have less memory and force a smaller zone database for the entire fabric.

Recommended Action

Execute the `cfgSize` command to view the zone database size information. Edit the zone database to keep it within the allowable limit for the specific switches in your fabric.

ZONE-1072**Message**

FSS sync failure due to Active CP <reason for sync failure>

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the standby zoning component received AD configuration from the primary side.

Recommended Action

To display the AD configuration use `ad --exec 255 "ad --show"` command or `ad --sel 255` command followed by `ad --show` command.

Synchronize the standby control processor (CP) using the `haSyncStart` command, after removing AD configuration on Active CP using `ad --delete` command followed by `ad --apply` command.

ZONE-1073

Message

<PID_1> device illegally zoned by port, and/or is zoned with device that is port zoned - affected PID pair (<PID_2>, <PID_3>).

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that an FCoE or FCLAG device is either port zoned, and/or is zoned with another device that is port zoned.

Recommended Action

Modify the zoning configuration so that devices are not port zoned with any FCoE or FCLAG device.

ZONE-1074

Message

Management Interface commit operation did not contain checksum field.

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the Management Interface commit operation did not contain a checksum field.

This can either indicate that a non-checksum-supporting Interface is connected or that a checksum-supporting interface failed to provide a checksum.

Recommended Action

No action is necessary. Users need to be aware that commit operations from non-checksum-supporting Management Interfaces may result in zoning data being overwritten with stale data.

Please note that this message is only issued upon detecting Checksum-to-NonChecksum transitions.

ZONE-1075

Message

Zone fabric lock timeout value has been changed by domain <Domain ID of switch that initiated the change.> (old <Old timeout value> mins, new <New timeout value> mins).

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that the zone fabric lock timeout value was changed.

Recommended Action

No action is necessary. Users need to be aware that the zone fabric lock timeout duration has been changed.

ZONE-1076

Message

Zone fabric lock has been canceled (Reason: <Reason for zone fabric lock cancellation.>)

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the zone fabric lock has been canceled unexpectedly.

Recommended Action

No action is necessary. Users need to be aware that the zone fabric lock has been cleared on the local switch.

ZONE-1077

Message

Zone commit from downlevel switch <Domain ID of downlevel switch that initiated the zone commit.> was blocked due to an active zone fabric lock

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the zone commit operation initiated from a downlevel switch was blocked due to there being an active zone fabric lock.

Recommended Action

No action is necessary. Users need to be aware that there is a downlevel switch in the fabric that does not support Zone Fabric Locking that is attempting to perform zone commit operations.

ZONE-1078**Message**

Compressed zone database size exceeds the maximum supported limit. (size <Compressed zone database size>, max <Maximum Information unit size>)

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the compressed size of the zone database has exceeded the maximum supported inter-switch Information unit size limit.

Recommended Action

Execute the `cfgSize` command to view the zone database size information. Reduce the zone database size and retry the operation

ZONE-1079**Message**

Zone merge failed due to fabric zone database size exceeding limits of switch attempting merge on port <port>

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the zone database size is greater than the limit allowed by the switch attempting zone merge on specified port. The limit of the zone database size depends on the lowest level switch in the fabric. Older switches have less memory and force a smaller zone database for the entire fabric.

Recommended Action

Execute the `cfgSize` command to view the zone database size information. Reduce the zone database size and reenoble the ISLs for the merge operation to be retried

ZONE-1080

Message

Traffic Isolation (TI) Zones have been detected and are deprecated in Fabric OS 9.0.0.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that Traffic Isolation (TI) zones have either been detected during reboot or were newly imported when there were none before.

Recommended Action

No action is necessary. Users need to be aware that Traffic Isolation (TI) zones have been deprecated and can no longer be created or edited in Fabric OS 9.0.0. Please refer to the Fabric OS Administrator's Guide for more information

ZONE-1081

Message

Frame Redirection (RD) Zones have been detected and are deprecated in Fabric OS 9.0.0.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that Frame Redirection (RD) zones have either been detected during reboot or were newly imported when there were none before.

Recommended Action

No action is necessary. Users need to be aware that Frame Redirection (RD) zones have been deprecated and can no longer be created or edited in Fabric OS 9.0.0. Please refer to the Fabric OS Administrator's Guide for more information.

ZONE-1082**Message**

LSAN zones size for configuration <Configuration name> has exceeded the maximum limit. (size <LSAN zones size>, max <Maximum Information unit size>)

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that the LSAN zones size for the zone configuration being enabled has exceeded the maximum inter-switch Information unit size limit.

Recommended Action

Reduce the size and/or number of LSAN zones in the zone configuration and retry the configuration Enable operation

ZONE-1083**Message**

Invalid peer zone (<Peer zone name>) detected in the zone database. (Reason: <Reason for bad peer zone>)

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that an invalid peer zone was detected in the zone database.

Recommended Action

Users should inspect the peer zone that was flagged as invalid and make the necessary zone database corrections.

ZONE-1084

Message

Zone fabric lock-principal domain conflict detected with domain <Domain ID of the switch that is in conflict.>.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that there was a zone fabric lock-principal merge conflict.

Recommended Action

Users should first check the zone transaction state on both switches using the `cfgTransShow` command.

Users should be aware that the zone fabric lock has been canceled and zone transactions will remain open as long as no other zone commit operation is performed by some other client. Users will want to perform either a zone edit or commit operation on the switch whose zone transaction they want to retain.

ZONE-1085

Message

Zone fabric lock timeout conflict detected with domain <Domain ID of the switch that is in conflict.> (local: <Local zone fabric lock timeout value.> mins, remote: <Remote zone fabric lock timeout value.> mins).

Message Type

LOG

Message Severity

INFO

Probable Cause

Indicates that there was a merge conflict with the zone fabric lock timeout value.

Recommended Action

Users are suggested to set a consistent timeout value using the `zoneFabricLock --timeout` command after the fabric is stable.

ZONE-1086

Message

Frame Redirection (RD) Zones detected in the configuration and are not supported in GEN7 Platforms.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that Frame Redirection (RD) zones are present in the configuration but will not be supported in GEN7 Platforms.

Recommended Action

Users need to be aware that Frame Redirection (RD) zones have been deprecated and will not be enforced in GEN7 platforms in Fabric OS 9.0.0. Please refer to the Fabric OS Administrator's Guide for more information.

ZONE-1087

Message

The zone update did not complete successfully.

Message Type

LOG | FFDC

Message Severity

WARNING

Probable Cause

Indicates that there was an error during the zone update from a remote domain. This switch's zone database may be out of sync with the rest of the switches in the fabric.

Recommended Action

Execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

ZONE-1088

Message

The defined zone database is empty while having an effective zone configuration.

Message Type

LOG | FFDC

Message Severity

WARNING

Probable Cause

Indicates that a bad zone database state was detected. This switch's zone database may be out of sync with the rest of the switches in the fabric.

Recommended Action

Execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

ZONE-1089**Message**

The zone message queue has reached <The zone message queue usage high/low threshold limit.> percent of its maximum limit.

Message Type

LOG | FFDC

Message Severity

WARNING

Probable Cause

Indicates that the zoning service is receiving events faster than it is able to process them and the zone message queue is nearing its maximum limit.

Recommended Action

Execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

ZONE-1090**Message**

Logical SAN (LSAN) Zones did not get propagated to the Fibre Channel router switch.

Message Type

LOG | FFDC

Message Severity

WARNING

Probable Cause

Indicates that there was an internal error that prevented LSAN zones from getting propagated to the Fibre Channel router switch.

Recommended Action

Execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

ZONE-1091

Message

A stale zone transaction with transaction id \"0x<Zone transaction ID>\" has been aborted.

Message Type

LOG

Message Severity

INFO

Probable Cause

The stale zone transaction has been aborted due to the transaction owner no longer being alive

ZONE-1092

Message

Invalid entry found in the zone database. \"<Invalid zone object member list>\"

Message Type

LOG

Message Severity

WARNING

Probable Cause

An unexpected semicolon was found in the zone database.

Recommended Action

Users should refrain from performing any further zoning operations from this switch and instead perform zoning operations from another switch that has a valid zone database.

Users should also execute the `supportFtp` (as needed) to set up automatic FTP transfers; then execute the `supportSave` and contact your switch service provider.

ZONE-1093

Message

Broadcast zones have been detected and are deprecated in Fabric OS 9.0.1.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that Broadcast zones have either been detected during reboot or were newly imported when there were none before.

Recommended Action

No action is necessary. Users need to be aware that Broadcast zones have been deprecated and can no longer be created or edited in Fabric OS 9.0.1. Please refer to the Fabric OS Administrator's Guide for more information

ZONE-1094

Message

The zone database flash file is corrupted.

Message Type

LOG | FFDC

Message Severity

ERROR

Probable Cause

Indicates that the zone configuration restored from flash memory was corrupted.

Recommended Action

If the problem persists, execute the `supportFtp` command (as needed) to set up automatic FTP transfers; then execute the `supportSave` command and contact your switch service provider.

ZONE-1095

Message

<Deprecated Zone Object Type> zones have been detected and are deprecated in Fabric OS.

Message Type

LOG

Message Severity

ERROR

Probable Cause

Indicates that there was an attempt to import a deprecated zone object.

Recommended Action

No action is necessary. Users need to be aware that the specified zone object type has been deprecated and is no longer supported in Fabric OS. Please refer to the Fabric OS Administrator's Guide for more information

ZONE-1096

Message

GMI timer has expired for ct <CT command name> [0x<Transaction Id>, 0x<Source ID (SID) of device that issued the CT command>].

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that a CT request has not received its outstanding GMI request within 60 seconds.

Recommended Action

Verify the device that issued the CT request is working properly and if the issue persists, capture the supportsave and contact the switch service provider.

ZONE-1097

Message

Zone database is outdated for the outstanding GMI requests.

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the zone database was updated while there was an outstanding GMI request.

Recommended Action

No action is needed. But users should be aware that any outstanding GMI exchanges initiated before the zone database was updated will become stale and will get rejected.

ZONE-1098**Message**

CT command <CT command name> [0x<Transaction Id>, 0x<Source ID (SID) of device that issued the CT command>] has exceeded the maximum number of retries (3) within the timeout period (60 seconds).

Message Type

LOG

Message Severity

WARNING

Probable Cause

Indicates that the same CT request has been sent more than the maximum number of allowable retries within a sixty second period.

Recommended Action

No action is needed. Users should be aware that devices are allowed to send a maximum of three duplicate CT requests for a transaction ID within the GMI timeout period (60 seconds). Any subsequent duplicate requests received within the sixty second period will be rejected.

ZONE-3001**Message**

Event: <Event Name>, Status: success, Info: <Zone object type> \"<Zone object member list>\" added to <Zone object set type> \"<Zone object set name>\".

Message Type

AUDIT

Message Class

ZONE

Message Severity

INFO

Probable Cause

Indicates that a new zone object member or members have been added to the specified zone object set.

The *zone object type* variable can be an alias, zone member, zone, or zone configuration. The string "..." appears at the end of the *zone object member list* variable if the list was truncated in the message.

Recommended Action

Verify that the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

ZONE-3002**Message**

Event: <Event Name>, Status: success, Info: <Zone object set type> \"<Zone object set name>\" created with <Zone object type> \"<Zone object member list>\".

Message Type

AUDIT

Message Class

ZONE

Message Severity

INFO

Probable Cause

Indicates that a new zone object set was created and the specified zone object member or members were added to the zone object set.

The *zone object type* variable can be an alias, zone member, zone, or zone configuration. The string "..." appears at the end of the *zone object member list* variable if the list was truncated in the message.

Recommended Action

Verify the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

ZONE-3003

Message

Event: <Event Name>, Status: success, Info: <Zone object type> \"<Zone object name>\" deleted.

Message Type

AUDIT

Message Class

ZONE

Message Severity

INFO

Probable Cause

Indicates that the specified zone object has been deleted.

The *zone object type* variable can be an alias, zone member, zone, or zone configuration.

Recommended Action

Verify that the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

ZONE-3004

Message

Event: <Event Name>, Status: success, Info: <Zone object type> \"<Zone object member list>\" removed from <Zone object set type> \"<Zone object set name>\".

Message Type

AUDIT

Message Class

ZONE

Message Severity

INFO

Probable Cause

Indicates that the specified zone object member or members have been removed from the specified zone object set.

The *zone object type* variable can be an alias, zone member, zone, or zone configuration. The string \"...\" appears at the end of the *zone object member list* variable if the list was truncated in the message.

Recommended Action

Verify the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

ZONE-3005**Message**

Event: <Event Name>, Status: success, Info: All zone information cleared from transaction buffer.

Message Type

AUDIT

Message Class

ZONE

Message Severity

INFO

Probable Cause

Indicates that all the zone information has been cleared from the transaction buffer.

Recommended Action

Verify that the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

ZONE-3006**Message**

Event: <Event Name>, Status: success, Info: Current zone configuration disabled. <AD Id>

Message Type

AUDIT

Message Class

ZONE

Message Severity

INFO

Probable Cause

Indicates that the current zone configuration has been disabled.

Recommended Action

Verify that the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

ZONE-3007**Message**

Event: <Event Name>, Status: success, Info: Zone configuration \"<Zone configuration>\" enabled. <AD Id>

Message Type

AUDIT

Message Class

ZONE

Message Severity

INFO

Probable Cause

Indicates that the specified zone configuration has been enabled.

Recommended Action

Verify that the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

ZONE-3008**Message**

Event: <Event Name>, Status: success, Info: Current zone configuration saved to MRAM. <AD Id>

Message Type

AUDIT

Message Class

ZONE

Message Severity

INFO

Probable Cause

Indicates that the current zone configuration has been successfully saved to magnetoresistive random access memory (MRAM).

Recommended Action

Verify that the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

ZONE-3009**Message**

Event: <Event Name>, Status: success, Info: <Event Description>.

Message Type

AUDIT

Message Class

ZONE

Message Severity

INFO

Probable Cause

Indicates that the specified zone transaction has been successful.

Recommended Action

Verify that the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

ZONE-3010**Message**

Event: <Event Name>, Status: success, Info: Zone object \"<Zone object name>\" copied to new zone object \"<New Zone object name>\".

Message Type

AUDIT

Message Class

ZONE

Message Severity

INFO

Probable Cause

Indicates that the specified zone object has been copied to a new zone object.

Recommended Action

Verify that the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

ZONE-3011**Message**

Event: <Event Name>, Status: success, Info: Zone object \"<Zone object name>\" expunged.

Message Type

AUDIT

Message Class

ZONE

Message Severity

INFO

Probable Cause

Indicates that the specified zone object has been expunged.

Recommended Action

Verify that the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

ZONE-3012**Message**

Event: <Event Name>, Status: success, Info: Zone object \"<Zone object name>\" renamed to \"<New Zone object name>\".

Message Type

AUDIT

Message Class

ZONE

Message Severity

INFO

Probable Cause

Indicates that the specified zone object has been renamed.

Recommended Action

Verify that the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

ZONE-3026**Message**

Event: <Event Name>, Status: success, Info: Zone object \"<Zone object name>\" replaced with \"<New Zone object name>\".

Message Type

AUDIT

Message Class

ZONE

Message Severity

INFO

Probable Cause

Indicates that the specified zone object has been replaced.

Recommended Action

Verify that the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

ZONE-3027**Message**

Target Driven Peer Zone commit configuration \"<Configuration name>\" completed successfully.

Message Type

AUDIT | LOG

Message Class

ZONE

Message Severity

INFO

Probable Cause

Indicates that the Target Driven Peer Zone configuration commit has been completed successfully.

Recommended Action

Verify that the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

ZONE-3028**Message**

Target Driven Peer Zone commit configuration <Failure and its reason if available>.

Message Type

AUDIT | LOG

Message Class

ZONE

Message Severity

ERROR

Probable Cause

Indicates that the Target Driven Peer Zone configuration commit has failed.

Recommended Action

Verify that the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

ZONE-3029**Message**

Target Driven Peer Zone \"<Zone name>\" add operation from device <WWN of the device which initiated the Target Driven Peer Zone add request> completed successfully.

Message Type

AUDIT

Message Class

ZONE

Message Severity

INFO

Probable Cause

Indicates that the Target Driven Peer Zone add operation has been completed successfully.

Recommended Action

Verify that the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

ZONE-3030**Message**

Target Driven Peer Zone \"<Zone name>\" replace operation from device <WWN of the device which initiated the Target Driven Peer Zone replace request> completed successfully.

Message Type

AUDIT

Message Class

ZONE

Message Severity

INFO

Probable Cause

Indicates that the Target Driven Peer Zone replace operation has been completed successfully.

Recommended Action

Verify that the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

ZONE-3031**Message**

Target Driven Peer Zone \"<Zone name>\" remove operation from device <WWN of the device which initiated the Target Driven Peer Zone remove request> completed successfully.

Message Type

AUDIT

Message Class

ZONE

Message Severity

INFO

Probable Cause

Indicates that the Target Driven Peer Zone remove operation has been completed successfully.

Recommended Action

Verify that the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

ZONE-3032**Message**

Target Driven Peer Zone \"<Zone name>\" add operation from device <WWN of the device which initiated the Target Driven Peer Zone add request> failed due to an error in <error description>.

Message Type

AUDIT | LOG

Message Class

ZONE

Message Severity

ERROR

Probable Cause

Indicates that the Target Driven Peer Zone add operation failed.

Recommended Action

Verify that the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

ZONE-3033**Message**

Target Driven Peer Zone \"<Zone name>\" replace operation from device <WWN of the device which initiated the Target Driven Peer Zone replace request> failed due to an error in <error description>.

Message Type

AUDIT | LOG

Message Class

ZONE

Message Severity

ERROR

Probable Cause

Indicates that the Target Driven Peer Zone replace operation failed.

Recommended Action

Verify that the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

ZONE-3034**Message**

Target Driven Peer Zone \"<Zone name>\" remove operation from device <WWN of the device which initiated the Target Driven Peer Zone remove request> failed due to an error in <error description>.

Message Type

AUDIT | LOG

Message Class

ZONE

Message Severity

ERROR

Probable Cause

Indicates that the Target Driven Peer Zone remove operation failed.

Recommended Action

Verify that the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

MAPS Monitoring Systems and RASLog IDs

This section maps the MAPS monitoring systems to their corresponding RASLog IDs.

Refer to the *Brocade® Fabric OS® MAPS User Guide* for more information about MAPS threshold values and actions.

Table 11: MAPS Monitoring System and RASLog IDs

Monitoring System	RASLOG IDs	Supported Platform
CRC errors (CRC)	MAPS-2004 to 2007	Fabric OS
Invalid transmit words (ITW)	MAPS-2008 to 2011	Fabric OS
Sync loss (LOSS_SYNC)	MAPS-2012 to 2015	Fabric OS
Link failure (LF)	MAPS-2016 to 2019	Fabric OS
Loss of signal (LOSS_SIGNAL)	MAPS-2020 to 2023	Fabric OS
Protocol errors (PE)	MAPS-2024 to 2027	Fabric OS
State change (STATE_CHG)	MAPS-2028 to 2031	Fabric OS
Link reset (LR)	MAPS-2032 to 2035	Fabric OS
C3 timeout (C3TXTO)	MAPS-2036 to 2039	Fabric OS
Receive errors per minute (RX)	MAPS-2040 to 2043	Fabric OS
Transmit errors per minute (TX)	MAPS-2044 to 2047	Fabric OS
Utility errors per minute (UTIL)	MAPS-2048 to 2051	Fabric OS
GE_CRC	MAPS-2060 to 2063	Fabric OS
GE_LOS_OF_SIG	MAPS-2064 to 2067	Fabric OS
Fabric Performance Impact (DEV_LATENCY_IMPACT)	MAPS-2068 to 2071	Fabric OS
DEV_NPIV_LOGINS	MAPS-2080 to 2083	Fabric OS
Block errors per minute (ENCR_BLK)	MAPS-2092 to 2095	Fabric OS
Discard errors per minute (ENCR_DISC)	MAPS-2096 to 2099	Fabric OS
Short frame errors per minute (ENCR_SHRT_FRM)	MAPS-2100 to 2103	Fabric OS
CRC	MAPS-2108 to 2111	Fabric OS
ITW	MAPS-2112 to 2115	Fabric OS
LR	MAPS-2116 to 2119	Fabric OS
BAD_OS	MAPS-2120 to 2123	Fabric OS
FRM_LONG	MAPS-2124 to 2127	Fabric OS
FRM_TRUNC	MAPS-2128 to 2131	Fabric OS
CIR_STATE	MAPS-2140 to 2143	Fabric OS
CIR_UTIL	MAPS-2144 to 2147	Fabric OS
CIR_PKTLOSS	MAPS-2148 to 2151	Fabric OS
Flash memory percentage used (FLASH_USAGE)	MAPS-2152 to 2155	Fabric OS
CPU percentage used (CPU)	MAPS-2156 to 2159	Fabric OS
Memory percentage used (MEMORY_USAGE)	MAPS-2160 to 2163	Fabric OS
Temperature sensor (TEMP)	MAPS-2164 to 2167	Fabric OS

Monitoring System	RASLOG IDs	Supported Platform
Power supply (PS_STATE)	MAPS-2168 to 2171	Fabric OS
Fan (FAN_STATE)	MAPS-2172 to 2175	Fabric OS
SFP (SFP_STATE)	MAPS-2180 to 2183	Fabric OS
Slot (BLADE_STATE)	MAPS-2184 to 2187	Fabric OS
WWN (WWN)	MAPS-2188 to 2191	Fabric OS
FAN_AIRFLOW_MISMATCH	MAPS-2192 to 2195	Fabric OS
Telnet violations (SEC_TELNET)	MAPS-2196 to 2199	Fabric OS
HTTP violation (SEC_HTTP)	MAPS-2200 to 2203	Fabric OS
SCC violations (SEC_SCC)	MAPS-2204 to 2207	Fabric OS
DCC violations (SEC_DCC)	MAPS-2208 to 2211	Fabric OS
Login violations (SEC_LV)	MAPS-2212 to 2215	Fabric OS
Invalid certifications (SEC_CERT)	MAPS-2216 to 2219	Fabric OS
TS out of sync (SEC_TS)	MAPS-2220 to 2223	Fabric OS
SLAP failures (SEC_AUTH_FAIL)	MAPS-2224 to 2227	Fabric OS
No FCS (SEC_FCS)	MAPS-2228 to 2231	Fabric OS
Incompatible security DB (SEC_IDB)	MAPS-2232 to 2235	Fabric OS
Illegal command (SEC_CMD)	MAPS-2236 to 2239	Fabric OS
Number of days to expire (DAYS_TO_EXPIRE)	MAPS-2240 to 2243	Fabric OS
Expired certifications (EXPIRED_CERTS)	MAPS-2244 to 2247	Fabric OS
Temperature (SFP_TEMP)	MAPS-2260 to 2263	Fabric OS
Voltage (VOLTAGE)	MAPS-2264 to 2267	Fabric OS
Current (CURRENT)	MAPS-2268 to 2271	Fabric OS
Receive power (RXP)	MAPS-2272 to 2275	Fabric OS
Transmit power (TXP)	MAPS-2276 to 2279	Fabric OS
PWR_HRS	MAPS-2280 to 2283	Fabric OS
BAD_TEMP	MAPS-2284 to 2287	Fabric OS
BAD_PWR	MAPS-2288 to 2291	Fabric OS
BAD_FAN	MAPS-2292 to 2295	Fabric OS
FAULTY_PORTS	MAPS-2296 to 2299	Fabric OS
MISSING_SFP	MAPS-2300 to 2303	Fabric OS
FAULTY_BLADE	MAPS-2304 to 2307	Fabric OS
MARG_PORTS	MAPS-2308 to 2311	Fabric OS
ERR_PORTS	MAPS-2312 to 2315	Fabric OS
E_Ports down (EPORT_DOWN)	MAPS-2316 to 2319	Fabric OS
Fabric reconfiguration (FAB_CFG)	MAPS-2320 to 2323	Fabric OS
Domain ID change (DID_CHG)	MAPS-2324 to 2327	Fabric OS
Segmentation changes (FAB_SEG)	MAPS-2328 to 2331	Fabric OS
Zone changes (ZONE_CHG)	MAPS-2336 to 2339	Fabric OS
Fabric logins (FLOGI)	MAPS-2340 to 2343	Fabric OS
L2 device count (L2_DEVCNT_PER)	MAPS-2344 to 2347	Fabric OS

Monitoring System	RASLOG IDs	Supported Platform
LSAN device count (LSAN_DEVCNT_PER)	MAPS-2348 to 2351	Fabric OS
Zone configuration size (ZONE_CFGSZ_PER)	MAPS-2352 to 2355	Fabric OS
FCR count (BB_FCR_CNT)	MAPS-2356 to 2359	Fabric OS
DOWN_CORE	MAPS-2360 to 2363	Fabric OS
HA_SYNC	MAPS-2364 to 2367	Fabric OS
WWN_DOWN	MAPS-2368 to 2371	Fabric OS
ETH_MGMT_PORT_STATE	MAPS-2408 to 2411	Fabric OS
TUNNEL_STATE	MAPS-2412 to 2415	Fabric OS
TUNNEL_UTIL	MAPS-2416 to 2419	Fabric OS
QoS utilization percentage (QOS_UTIL)	MAPS-2420 to 2423	Fabric OS
QoS packet loss percentage (PKTLOSS)	MAPS-2424 to 2427	Fabric OS
Circuit round-trip times (RTT)	MAPS-2428 to 2431	Fabric OS
Circuit jitter (JITTER)	MAPS-2432 to 2439	Fabric OS
Circuit QoS utilization percentage (CIR_QOS_UTIL)	MAPS-2440 to 2443	Fabric OS
Circuit QoS packet loss percentage (CIR_QOS_PKTLOSS)	MAPS-2444 to 2447	Fabric OS
RD_PENDING_IO	MAPS-2992 to 2995	Fabric OS
WR_PENDING_IO	MAPS-2996 to 2999	Fabric OS
VTAP_IOPS	MAPS-2668 to 2671	Fabric OS
BE_LATENCY_IMPACT	MAPS-2672 to 2675	Fabric OS
TUNNEL_IP_UTIL	MAPS-2700 to 2703	Fabric OS
CIR_IP_UTIL	MAPS-2704 to 2707	Fabric OS
CIR_IP_PKTLOSS	MAPS-2708 to 2711	Fabric OS
IP_RTT	MAPS-2712 to 2715	Fabric OS
IP_JITTER	MAPS-2716 to 2719	Fabric OS
IT_FLOW	MAPS-2936 to 2939	Fabric OS
AVG_PENDING_IOS	MAPS-2940 to 2943	Fabric OS
MAX_PENDING_IOS	MAPS-2944 to 2947	Fabric OS
MAX_ROS	MAPS-2948 to 2951	Fabric OS
AVG_ROS	MAPS-2952 to 2955	Fabric OS
IP_EXTN_FLOW	MAPS-2956 to 2959	Fabric OS
SFP_STATE	MAPS-3000 to 3003	Fabric OS
DEV_LOGIN_DIST	MAPS-3004 to 3007	Fabric OS
SYSTEM_TEMP	MAPS-3024 to 3027	Fabric OS
PORT_BANDWIDTH	MAPS-3036 to 3039	Fabric OS
MARG_SFPS	MAPS-3040 to 3043	Fabric OS
TRUFOS_CERT_DAYS_TO_EXPIRE	MAPS-3052 to 3055	Fabric OS
TRUFOS_CERT_EXPIRED	MAPS-3056 to 3059	Fabric OS
ASC_UPLOAD_FAILURE	MAPS-3060 to 3063	Fabric OS
MAX_RD_PENDING_IO	MAPS-3064 to 3067	Fabric OS

Monitoring System	RASLOG IDs	Supported Platform
MAX_WR_PENDING_IO	MAPS-3068 to 3071	Fabric OS
IO_TIMEOUT	MAPS-3072 to 3075	Fabric OS
IO_ERROR	MAPS-3088 to 3091	Fabric OS
MAX_RD_PENDING_IO	MAPS-3092 to 3095	Fabric OS
MAX_WR_PENDING_IO	MAPS-3096 to 3099	Fabric OS
RD_1stDATA_TIME_VIOL	MAPS-3120 to 3123	Fabric OS
WR_1stXFER_RDY_VIOL	MAPS-3124 to 3127	Fabric OS
RD_STATUS_TIME_VIOL	MAPS-3128 to 3131	Fabric OS
WR_STATUS_TIME_VIOL	MAPS-3132 to 3135	Fabric OS
ROUTING_ERR	MAPS-3136 to 3139	Fabric OS
TRUFOS_CERT_INSTALLED	MAPS-3140 to 3143	Fabric OS
IO_ABORT	MAPS-3144 to 3147	Fabric OS
RESERVE	MAPS-3148 to 3151	Fabric OS
MEMORY_USAGE_STATE	MAPS-3152 to 3155	Fabric OS
STATE_CHG	MAPS-3156 to 3159	Fabric OS

Revision History

The revision history provides a list of the significant changes made in each version of the document.

FOS-92x-Message-RM101; June 30, 2023

Messages that were added:

- C5-1057
- GE5-1057
- SEC-1352
- SEC-3097

FOS-92x-Message-RM100; April 28, 2023

Initial document version.

Documentation Legal Notice

This notice provides copyright and trademark information as well as legal disclaimers.

Copyright © 2023. Broadcom. All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries. For more information, go to www.broadcom.com. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

Broadcom reserves the right to make changes without further notice to any products or data herein to improve reliability, function, or design. Information furnished by Broadcom is believed to be accurate and reliable. However, Broadcom does not assume any liability arising out of the application or use of this information, nor the application or use of any product or circuit described herein, neither does it convey any license under its patent rights nor the rights of others.

The product described by this document may contain open source software covered by the GNU General Public License or other open source license agreements. To find out which open source software is included in Brocade products or to view the licensing terms applicable to the open source software, please download the open source attribution disclosure document in the Broadcom Support Portal. If you do not have a support account or are unable to log in, please contact your support provider for this information.

