Extreme SLX-OS
Message Reference, 20.7.3

Supporting ExtremeRouting and ExtremeSwitching
SLX 9740, SLX 9640, SLX 9540, SLX 9250, SLX 9150,
Extreme 8820, Extreme 8720, and Extreme 8520

9039525-00 Rev AB
November 2026



Copyright © 2026 Extreme Networks, Inc. All rights reserved.

Legal Notice

Extreme Networks, Inc. reserves the right to make changes in specifications and other information contained in this document and its website without prior notice. The reader should in all cases consult representatives of Extreme Networks to determine whether any such changes have been made.

The hardware, firmware, software or any specifications described or referred to in this document are subject to change without notice.

Trademarks

Extreme Networks and the Extreme Networks logo are trademarks or registered trademarks of Extreme Networks, Inc. in the United States and/or other countries.

All other names (including any product names) mentioned in this document are the property of their respective owners and may be trademarks or registered trademarks of their respective companies/owners.

For additional information on Extreme Networks trademarks, see: https://www.extremenetworks.com/about-extreme-networks/company/legal/trademarks

Open Source Declarations

Some software files have been licensed under certain open source or third-party licenses. End-user license agreements and open source declarations can be found at: https://www.extremenetworks.com/support/policies/open-source-declaration/

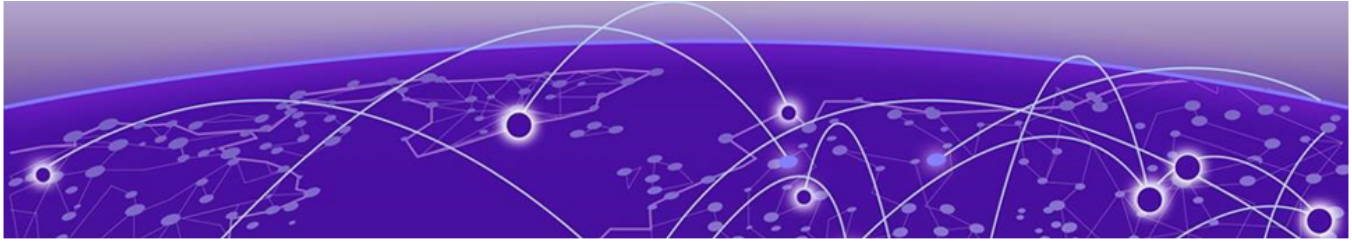


Table of Contents

Preface **32**
- Text Conventions 32
- Documentation and Training 33
  - Open Source Declarations 34
  - Training 34
- Help and Support 34
  - Subscribe to Product Announcements 35
- Send Feedback 35

About This Document **36**
- What's New in this Document 36
- Supported Hardware 36

SLX-OS Messaging **38**
- Overview of RASLog messages 38
  - RASLog message types 39
  - Message severity levels 41
  - RASLog message logging 41
- Configuring the syslog message destinations 42
  - System logging daemon 42
  - System console 44
  - SNMP management station 44
- Configuring the SNMP server hosts 45
  - Configuring the SNMP (version 1 or version 2c) server host 46
  - Configuring the SNMPv3 server 47
- Commands for displaying, clearing, and configuring the message logs 49
- Displaying message content on the switch 50
- Configuring system messages 51
  - Disabling a RASLog message or module 51
  - Enabling a RASLog message or module 51
  - Setting the severity level of a RASLog message 52
- Viewing and clearing the RASLog messages 52
  - Displaying the RASLog messages 52
  - Displaying the messages on an interface module 53
  - Clearing the RASLog messages 54
  - Viewing and clearing the SYSTEM messages 54
  - Viewing and clearing the DCE messages 54
  - Displaying the FFDC messages 55
  - Displaying the description of the RASLog modules 55
  - Displaying RASLog messages in a module 56
- Viewing, clearing, and configuring AUDIT log messages 56
  - Displaying the AUDIT messages 56

Clearing the AUDIT messages....59
Configuring event auditing....59
Understanding RASLog messages....59
RASLog messages....59
AUDIT event messages....61
Responding to a RASLog message....62
Gathering information about the problem....62
Support....63
System module descriptions....64
SLX-OS Modules....69
ARP Messages....70
ARP-1042....70
ARP-1043....71
AUTH Messages....71
AUTH-1001....71
AUTH-1002....71
AUTH-1003....72
AUTH-1004....72
AUTH-1006....72
AUTH-1007....73
AUTH-1010....73
AUTH-1012....73
AUTH-1013....73
AUTH-1014....74
AUTH-1017....74
AUTH-1018....74
AUTH-1020....75
AUTH-1022....75
AUTH-1025....75
AUTH-1026....76
AUTH-1027....76
AUTH-1028....76
AUTH-1029....77
AUTH-1030....77
AUTH-1031....78
AUTH-1032....78
AUTH-1033....78
AUTH-1034....79
AUTH-1035....79
AUTH-1036....79
AUTH-1037....80
AUTH-1039....80
AUTH-1040....80
AUTH-1041....81
AUTH-1042....81
AUTH-1044....82
AUTH-3001....82
AUTH-3002....82
AUTH-3004....83

AUTH-3005....83
AUTH-3006....83
AUTH-3007....84
AUTH-3008....84
BFD Messages....85
BFD-1001....85
BFD-1002....85
BFD-1005....86
BFD-1006....86
BFD-1007....86
BFD-1008....86
BFD-1009....87
BFD-1010....87
BGP Messages....87
BGP-1001....87
BGP-1002....88
BGP-1003....88
BGP-1004....88
BGP-1005....88
BGP-1006....89
BGP-1007....89
BGP-1009....89
BGP-1011....89
BGP-1012....90
BGP-1013....90
BGP-1014....90
BGP-1018....90
BGP-1019....91
BGP-1020....91
BGP-1021....91
BGP-1022....91
BGP-1023....92
BGP-1024....92
BGP-1025....92
BGP-1026....92
BGP-1027....93
BGP-1028....93
BGP-1029....93
BGP-1031....93
BGP-1032....94
BGP-1033....94
BGP-1034....94
BL Messages....94
BL-1000....94
BL-1001....95
BL-1002....95
BL-1003....95
BL-1004....96
BL-1006....96

BL-1007 97
BL-1008 97
BL-1009 97
BL-1010 98
BL-1011 98
BL-1012 99
BL-1013 99
BL-1014 100
BL-1015 100
BL-1016 101
BL-1017 101
BL-1018 101
BL-1019 102
BL-1020 102
BL-1021 102
BL-1022 103
BL-1023 103
BL-1024 103
BL-1026 104
BL-1027 104
BL-1028 104
BL-1029 105
BL-1031 105
BL-1032 105
BL-1033 106
BL-1034 106
BL-1037 106
BL-1038 107
BL-1039 107
BL-1045 107
BL-1046 108
BL-1047 108
BL-1049 108
BL-1050 109
BL-1051 109
BL-1052 109
BLL Messages 110
BLL-1000 110
CHS Messages 111
CHS-1002 111
CHS-1003 111
CHS-1004 111
CHS-1005 112
DAD Messages 112
DAD-1300 112
DAD-1301 112
DAD-1302 113
DAD-1303 113
DAD-1304 113

DAD-1305 113
DAD-1306 114
DAD-1307 114
DAD-1308 114
DAD-1309 114
DAD-1310 115
DAD-1311 115
DAD-1312 115
DAD-1313 115
DAD-1314 116
DAD-1315 116
DAD-1316 116
DAD-1317 116
DAD-1318 117
DAD-1319 117
DAD-1320 117
DAD-1321 117
DAD-1322 118
DAD-1323 118
DAD-1324 118
DAD-1325 118
DAD-1326 119
DAD-1327 119
DAD-1328 119
DAD-1329 119
DAD-1330 120
DAD-1340 120
DAD-1341 120
DAD-1342 120
DCM Messages 121
DCM-1002 121
DCM-1003 121
DCM-1004 121
DCM-1005 121
DCM-1006 122
DCM-1007 122
DCM-1008 122
DCM-1013 122
DCM-1014 123
DCM-1015 123
DCM-1016 123
DCM-1101 123
DCM-1102 124
DCM-1103 124
DCM-1104 124
DCM-1105 125
DCM-1106 125
DCM-1107 125
DCM-1108 125

DCM-1109 126
DCM-1110 126
DCM-1111 126
DCM-1112 126
DCM-1113 127
DCM-1114 127
DCM-1115 127
DCM-1116 127
DCM-1117 128
DCM-1118 128
DCM-1119 128
DCM-1120 128
DCM-1123 129
DCM-1124 129
DCM-1125 129
DCM-1126 129
DCM-1127 130
DCM-1128 130
DCM-1129 130
DCM-1201 130
DCM-1204 131
DCM-1205 131
DCM-1206 131
DCM-1207 131
DCM-1208 132
DCM-1209 132
DCM-1210 132
DCM-1211 132
DCM-1212 133
DCM-1301 133
DCM-1401 133
DCM-1402 133
DCM-1403 134
DCM-1457 134
DCM-1458 134
DCM-1471 135
DCM-1472 135
DCM-1473 135
DCM-1474 135
DCM-1475 136
DCM-2001 136
DCM-2002 136
DCM-3005 136
DCM-3010 137
DCM-3051 137
DCM-3052 137
DCM-3053 138
DCM-3054 138
DCM-3055 138

DCM-3056 138
DCM-3100 139
DCM-3101 139
DCM-4001 139
DCM-4002 139
DOT1 Messages 140
DOT1-1001 140
DOT1-1002 140
DOT1-1003 140
DOT1-1004 140
DOT1-1005 141
DOT1-1006 141
DOT1-1007 141
DOT1-1008 141
DOT1-1009 142
DOT1-1010 142
DOT1-1011 142
DOT1-1012 142
DOT1-1013 143
DOT1-1014 143
DOT1-1014 143
DOT1-1015 143
ELD Messages 144
ELD-1001 144
ELD-1002 144
ELD-1003 144
ELD-1004 145
ELD-1005 145
ELD-1006 145
ELD-1007 145
ELD-1008 146
ELD-1009 146
ELD-1010 146
ELD-1011 147
EM Messages 147
EM-1001 147
EM-1002 147
EM-1003 148
EM-1004 148
EM-1005 148
EM-1006 149
EM-1008 149
EM-1009 149
EM-1010 150
EM-1011 150
EM-1012 150
EM-1013 151
EM-1014 151
EM-1015 151

EM-1016 151
EM-1020 152
EM-1021 152
EM-1022 152
EM-1023 153
EM-1024 153
EM-1028 153
EM-1029 154
EM-1031 154
EM-1032 154
EM-1033 155
EM-1034 155
EM-1036 155
EM-1037 156
EM-1038 156
EM-1039 156
EM-1042 157
EM-1043 157
EM-1045 157
EM-1046 158
EM-1047 158
EM-1048 158
EM-1049 159
EM-1050 159
EM-1051 159
EM-1059 159
EM-1064 160
EM-1068 160
EM-1069 160
EM-1070 161
EM-1080 161
EM-1100 161
EM-1101 162
EM-1102 162
EM-1103 162
EM-1104 162
EM-2003 163
ERCP Messages 163
ERCP-1000 163
FABS Messages 163
FABS-1001 163
FABS-1002 164
FABS-1004 164
FABS-1005 164
FABS-1006 165
FABS-1007 165
FABS-1008 166
FABS-1009 166
FABS-1010 166

FABS-1011 166
FABS-1013 167
FABS-1014 167
FABS-1015 168
FSS Messages 168
FSS-1001 168
FSS-1002 168
FSS-1003 169
FSS-1004 169
FSS-1005 169
FSS-1006 169
FSS-1007 170
FSS-1008 170
FSS-1009 170
FSS-1010 171
FSS-1011 171
FSS-1012 171
FSS-1013 171
FSS-1014 172
FW Messages 172
FW-1001 172
FW-1002 172
FW-1003 173
FW-1004 173
FW-1005 173
FW-1006 174
FW-1007 174
FW-1008 174
FW-1009 175
FW-1010 175
FW-1012 175
FW-1034 176
FW-1035 176
FW-1036 176
FW-1038 176
FW-1039 177
FW-1040 177
FW-1042 177
FW-1043 178
FW-1044 178
FW-1046 179
FW-1047 179
FW-1048 179
FW-1050 179
FW-1051 180
FW-1052 180
FW-3101 180
FW-3102 181
FW-3103 181

FW-3104 181
FW-3105 182
FW-3107 182
FW-3108 182
FW-3109 183
FW-3110 183
FW-3111 183
FW-3113 184
FW-3114 184
FW-3115 184
FW-3116 185
FW-3117 185
FW-3119 185
FW-3120 186
FW-3121 186
FW-3122 186
FW-3123 187
FW-1297 187
FW-1298 187
FW-1299 188
FW-1341 188
FW-1342 188
FW-1343 188
FW-1403 189
FW-1404 189
FW-1405 189
FW-1406 190
FW-1407 190
FW-1408 190
FW-1409 190
FW-1410 191
FW-1411 191
FW-1412 191
FW-1413 191
FW-1414 192
FW-1415 192
FW-1424 192
FW-1425 192
FW-1426 193
FW-1427 193
FW-1428 193
FW-1429 194
FW-1430 194
FW-1431 194
FW-1432 194
FW-1433 195
FW-1434 195
FW-1447 196
FW-1435 196

FW-1439 196
FW-1440 196
FW-1441 197
FW-1442 197
FW-1443 197
FW-1444 198
FW-1500 198
FW-1501 198
FW-1510 198
FW-1511 199
FW-1512 199
HASM Messages 199
HASM-1000 199
HASM-1002 200
HASM-1003 200
HASM-1004 200
HASM-1013 201
HASM-1014 202
HASM-1015 202
HASM-1016 202
HASM-1020 202
HASM-1021 203
HASM-1022 203
HASM-1026 203
HASM-1027 203
HASM-1028 204
HASM-1029 204
HASM-1030 204
HASM-1105 205
HASM-1108 205
HASM-1109 205
HASM-1110 206
HASM-1111 206
HASM-1120 206
HASM-1121 206
HASM-1134 207
HASM-1200 207
HASM-1201 207
HASM-1202 207
HIL Messages 208
HIL-1202 208
HIL-1301 208
HIL-1302 208
HIL-1404 209
HIL-1405 209
HIL-1406 209
HIL-1407 209
HIL-1408 210
HIL-1409 210

HIL-1410 ... 210
HIL-1505 ... 210
HIL-1506 ... 211
HIL-1510 ... 211
HIL-1511 ... 211
HIL-1512 ... 212
HIL-1514 ... 212
HIL-1515 ... 212
HIL-1516 ... 213
HIL-1517 ... 213
HIL-1518 ... 214
HIL-1521 ... 214
HIL-1522 ... 214
HIL-1523 ... 215
HIL-1524 ... 215
HIL-1531 ... 216
HIL-1532 ... 216
HIL-1533 ... 216
HIL-1605 ... 217
HIL-1700 ... 217
HIL-1701 ... 217
HSL Messages ... 218
HSL-1000 ... 218
HSL-1001 ... 218
HSL-1004 ... 218
HSL-1006 ... 219
HSL-1009 ... 219
HSL-1010 ... 219
HSL-1011 ... 219
HSL-1020 ... 220
HSL-1021 ... 220
HSL-1022 ... 220
HSL-1023 ... 220
HSL-1024 ... 221
HSL-1025 ... 221
HSL-1026 ... 221
HSL-1027 ... 221
HSL-1028 ... 222
HSL-1029 ... 222
HSL-1030 ... 222
HSL-1031 ... 222
HSL-1032 ... 223
HSL-1033 ... 223
HSL-1034 ... 223
HSL-1052 ... 223
HSL-1061 ... 224
HSL-1062 ... 224
HSL-1069 ... 224
HSL-1070 ... 225

HSL-1071 225
HSL-1072 225
IGMP Messages 226
IGMP-1001 226
IGMP-1002 226
IGMP-1004 226
IGMP-1005 226
IGMP-1006 227
IPAD Messages 227
IPAD-1000 227
IPAD-1001 227
IPAD-1002 228
IPAD-1003 228
IPAD-1004 228
IPAD-1005 228
IPAD-1006 229
IPHL Messages 229
IPHL-1001 229
IPHL-1002 229
IPHL-1003 230
IPHL-1004 230
IPHL-1005 230
IPHL-1006 230
IPHL-1007 231
IPHL-1008 231
KTRC Messages 231
KTRC-1001 231
KTRC-1002 232
KTRC-1003 232
KTRC-1004 232
KTRC-1005 232
L2AG Messages 233
L2AG-1001 233
L2AG-1002 233
L2AG-1003 233
L2AG-1004 233
L2AG-1005 234
L2AG-1006 234
L2AG-1007 234
L2AG-1008 234
L2AG-1009 235
L2AG-1010 235
L2AG-1011 235
L2SS Messages 236
L2SS-1001 236
L2SS-1002 236
L2SS-1003 236
L2SS-1004 236
L2SS-1005 237

L2SS-1008 237
L2SS-1009 237
L2SS-1010 237
L2SS-1011 238
L2SS-1012 238
L2SS-1013 238
L2SS-1014 238
L2SS-1015 239
L2SS-1016 239
L2SS-1017 239
L2SS-1018 239
L2SS-1019 240
L2SS-1020 240
L2SS-1021 240
L2SS-1022 240
L2SS-1024 241
L2SS-1025 241
L2SS-1026 241
L2SS-1027 241
L2SS-1028 242
L2SS-1029 242
L2SS-1031 242
L2SS-1036 242
L2SS-1037 243
LACP Messages 243
LACP-1001 243
LACP-1002 243
LACP-1003 244
LACP-1004 244
LACP-1005 244
LACP-1006 244
LIC Messages 245
LIC-1001 245
LIC-1002 245
LIC-1003 245
LIC-1004 245
LIC-1005 246
LIC-1006 246
LIC-1015 246
LOG Messages 246
LOG-1000 246
LOG-1001 247
LOG-1002 247
LOG-1003 247
LOG-1004 247
LOG-1005 248
LOG-1006 248
LOG-1007 248
LOG-1008 249

LOG-1009 249
LOG-1010 249
LOG-1011 249
LOG-1012 250
MAPS Messages 250
MAPS-1001 250
MAPS-1002 250
MAPS-1003 251
MAPS-1004 251
MAPS-1010 251
MAPS-1011 251
MAPS-1012 252
MAPS-1020 252
MAPS-1021 252
MAPS-1100 253
MAPS-1101 253
MAPS-1102 253
MAPS-1110 253
MAPS-1111 254
MAPS-1112 254
MAPS-1113 254
MAPS-1114 254
MAPS-1115 255
MAPS-1116 255
MAPS-1120 255
MAPS-1121 256
MAPS-1122 256
MAPS-1123 256
MAPS-1124 256
MAPS-1125 257
MAPS-1126 257
MAPS-1127 257
MAPS-1130 257
MAPS-1131 258
MAPS-1132 258
MAPS-1200 258
MAPS-1201 259
MAPS-1202 259
MAPS-1203 259
MCST Messages 259
MCST-1001 259
MCST-1002 260
MCST-1003 260
MCST-1004 260
MCST-1005 261
MCST-1006 261
MCST-1007 261
MCST-1008 261
MCST-1009 262

MCST-1010 262
MCST-1011 262
MCST-1012 262
MCST-1013 263
MCST-1014 263
MCST-1015 263
MCST-1016 263
MCST-1017 264
MCST-1018 264
MCST-1019 264
MCST-1020 264
MM Messages 265
MM-1001 265
MPTH Messages 265
MPTH-1001 265
MPTH-1002 265
MPTH-1003 265
MSTP Messages 266
MSTP-1001 266
MSTP-1002 266
MSTP-1003 266
MSTP-1004 267
MSTP-2001 267
MSTP-2002 267
MSTP-2003 268
MSTP-2004 268
MSTP-2005 268
MSTP-2006 268
MSTP-2007 269
MSTP-3003 269
NSM Messages 269
NSM-1001 269
NSM-1002 269
NSM-1003 270
NSM-1004 270
NSM-1007 270
NSM-1009 270
NSM-1010 271
NSM-1011 271
NSM-1012 271
NSM-1013 271
NSM-1014 272
NSM-1015 272
NSM-1016 272
NSM-1017 272
NSM-1018 273
NSM-1019 273
NSM-1020 273
NSM-1021 273

NSM-1022 274
NSM-1026 274
NSM-1027 274
NSM-1028 274
NSM-1029 275
NSM-1030 275
NSM-1031 275
NSM-1032 275
NSM-1033 276
NSM-1034 276
NSM-1035 276
NSM-1036 276
NSM-1037 277
NSM-1038 277
NSM-1039 277
NSM-1040 277
NSM-1041 278
NSM-1042 278
NSM-1043 278
NSM-1044 278
NSM-1045 279
NSM-1046 279
NSM-1047 279
NSM-1048 279
NSM-1049 280
NSM-1050 280
NSM-1051 280
NSM-1052 280
NSM-1053 281
NSM-1062 281
NSM-1063 281
NSM-1064 281
NSM-1700 282
NSM-1701 282
NSM-1702 282
NSM-1703 282
NSM-2000 283
NSM-2001 283
NSM-2002 283
NSM-2003 283
NSM-2004 284
NSM-2005 284
NSM-2006 284
NSM-2007 284
NSM-2008 285
NSM-2010 285
NSM-2011 285
NSM-2012 286
NSM-2013 286

NSM-2014 286
NSM-2015 286
NSM-2016 287
NSM-2017 287
NSM-2018 287
NSM-2019 287
NSM-2020 288
NSM-2021 288
NSM-2022 288
NSM-2023 288
NSM-2024 289
NSM-2025 289
NSM-2026 289
NSM-2027 289
NSM-2028 290
NSM-2029 290
NSM-2030 290
NSM-2031 291
NSM-2032 291
NSM-2033 291
NSM-2034 291
NSM-2035 291
NSM-2036 292
NSM-2037 292
NSM-2038 292
NSM-2039 293
NSM-2040 293
NSM-2041 293
NSM-2042 293
NSM-2043 294
NSM-2044 294
NSM-2045 294
NSM-2046 294
NSM-2047 295
NSM-2048 295
NSM-2049 295
NSM-2050 295
NSM-2051 296
NSM-2052 296
NSM-2053 296
NSM-2071 297
NSM-2072 297
NSM-2073 297
NSM-2074 297
NSM-2075 297
NSM-2076 298
NSM-3001 298
NSM-3002 298
NSM-3003 298

NSM-3004 299
NSM-3005 299
NSM-3006 299
NSM-3007 299
NSM-3008 300
NSM-4000 300
OFMA Messages 300
OFMA-1001 300
OFD Messages 300
OFD-1001 300
OFD-1002 301
OFD-1003 301
OFD-2000 301
OFD-3000 301
OFD-3001 302
ONMD Messages 302
ONMD-1000 302
ONMD-1001 302
ONMD-1002 302
ONMD-1003 303
ONMD-1004 303
ONMD-1005 303
ONMD-1006 303
ONMD-1007 304
ONMD-1008 304
OSPF Messages 304
OSPF-1001 304
OSPF-1002 305
OSPF-1003 305
OSPF-1004 305
OSPF-1005 305
OSPF6 Messages 306
OSPF6-1001 306
OSPF6-1002 306
OSPF6-1003 306
PCAP Messages 306
PCAP-1001 306
PCAP-1002 307
PCAP-1003 307
PCAP-1004 307
PDM Messages 307
PDM-1001 307
PDM-1003 308
PDM-1004 308
PDM-1006 308
PDM-1007 309
PDM-1009 309
PDM-1010 309
PDM-1011 310

PDM-1012 310
PDM-1013 310
PDM-1014 311
PDM-1017 311
PDM-1019 311
PDM-1021 311
PHP Messages 312
PHP-1001 312
PHP-1002 312
PHP-1003 312
PHP-1004 312
PIM Messages 313
PIM-1001 313
PIM-1002 313
PLAT Messages 313
PLAT-1000 313
PLAT-1001 314
PLAT-1002 314
PLAT-1004 314
PLAT-1005 315
PLAT-1006 315
PLAT-1007 315
PLAT-1008 315
PLAT-1009 316
PLAT-1011 316
PLAT-1012 316
PLAT-1013 317
PLAT-1014 317
PORT Messages 317
PORT-1003 317
PORT-1004 318
PORT-1011 318
PORT-1012 319
PORT-1013 319
PORT-1014 319
PORT-1015 319
PORT-1016 320
PORT-1017 320
QOSD Messages 320
QOSD-1000 320
QOSD-1001 320
QOSD-1005 321
QOSD-1006 321
QOSD-1007 321
QOSD-1008 321
QOSD-1500 322
QOSD-1501 322
QOSD-1502 322
QOSD-1503 323

QOSD-1600 ... 323
QOSD-1601 ... 323
QOSD-1700 ... 323
QOSD-1800 ... 324
QOSD-1801 ... 324
RADV Messages ... 324
RADV-1001 ... 324
RADV-1002 ... 325
RADV-1003 ... 325
RADV-1004 ... 325
RADV-1005 ... 325
RADV-1006 ... 326
RADV-1007 ... 326
RADV-1008 ... 326
RADV-1009 ... 326
RADV-1010 ... 327
RADV-1011 ... 327
RADV-1006 ... 327
RAS Messages ... 328
RAS-1001 ... 328
RAS-1002 ... 328
RAS-1004 ... 328
RAS-1005 ... 328
RAS-1006 ... 329
RAS-1007 ... 329
RAS-1008 ... 329
RAS-2001 ... 329
RAS-2002 ... 330
RAS-2003 ... 330
RAS-2004 ... 330
RAS-2005 ... 331
RAS-2006 ... 331
RAS-2007 ... 331
RAS-3001 ... 331
RAS-3002 ... 332
RAS-3003 ... 332
RAS-3004 ... 332
RAS-3005 ... 332
RAS-3006 ... 333
RAS-3007 ... 333
RAS-3008 ... 333
RAS-3009 ... 333
RPS Messages ... 334
RPS-1001 ... 334
RPS-1750 ... 334
RPS-1751 ... 334
RPS-1752 ... 335
RPS-1753 ... 335
RPS-1754 ... 335

RTM Messages....335
RTM-1001....335
RTM-1002....336
RTM-1022....336
RTM-1032....336
RTM-1033....336
RTM-1037....337
RTM-1039....337
RTM-1040....337
RTM-1041....338
RTM-1042....338
SCN Messages....338
SCN-1001....338
SEC Messages....339
SEC-1033....339
SEC-1034....339
SEC-1036....340
SEC-1037....340
SEC-1044....340
SEC-1071....340
SEC-1180....341
SEC-1181....341
SEC-1184....341
SEC-1185....341
SEC-1187....342
SEC-1189....342
SEC-1190....343
SEC-1191....343
SEC-1192....343
SEC-1193....344
SEC-1197....344
SEC-1199....344
SEC-1203....344
SEC-1204....345
SEC-1205....345
SEC-1206....345
SEC-1307....346
SEC-1308....346
SEC-1312....346
SEC-1313....346
SEC-1325....347
SEC-1329....347
SEC-1334....347
SEC-1335....348
SEC-1336....348
SEC-1337....348
SEC-1338....348
SEC-1339....349
SEC-1340....349

SEC-1341 349
SEC-1342 349
SEC-1343 350
SEC-3014 350
SEC-3016 350
SEC-3018 351
SEC-3019 351
SEC-3020 351
SEC-3021 352
SEC-3022 352
SEC-3023 352
SEC-3024 353
SEC-3025 353
SEC-3026 353
SEC-3027 354
SEC-3028 354
SEC-3030 354
SEC-3034 355
SEC-3035 355
SEC-3036 355
SEC-3037 356
SEC-3038 356
SEC-3039 356
SEC-3045 357
SEC-3046 357
SEC-3049 357
SEC-3051 358
SEC-3061 358
SEC-3062 358
SEC-3067 358
SEC-3068 359
SEC-3069 359
SEC-3070 359
SEC-3071 360
SEC-3072 360
SEC-3073 360
SEC-3074 361
SEC-3075 361
SEC-3076 361
SEC-3077 362
SEC-3078 362
SEC-3079 362
SEC-3080 363
SEC-3081 363
SEC-3082 363
SEC-3083 364
SEC-3084 364
SEC-3085 364
SEC-3086 365

SEC-3087 365
SEC-3088 365
SEC-3089 366
SEC-3090 366
SEC-3091 366
SEC-3092 367
SEC-3093 367
SEC-3094 367
SEC-3095 368
SEC-3096 368
SEC-3097 368
SEC-3098 369
SEC-3099 369
SEC-3100 369
SEC-3101 370
SEC-3102 370
SEC-3103 370
SEC-3104 371
SEC-3105 371
SEC-3106 371
SEC-3107 372
SEC-3108 372
SEC-3110 372
SEC-3111 373
SEC-3112 373
SEC-3113 373
SEC-3136 374
SEC-3137 374
SEC-3138 374
SEC-3139 374
SEC-3140 375
SEC-3141 375
SEC-3142 375
SEC-3501 376
SEC-4002 376
SFLO Messages 376
SFLO-1001 376
SFLO-1002 376
SFLO-1003 377
SFLO-1004 377
SFLO-1005 377
SFLO-1006 377
SFLO-1007 378
SFLO-1008 378
SFLO-1009 378
SFLO-1010 379
SFLO-1011 379
SFLO-1012 379
SFLO-1013 379

SFLO-1014 380
SFLO-1015 380
SFLO-1016 380
SFLO-1017 380
SFLO-1018 380
SFLO-1019 381
SFLO-1021 381
SFLO-1022 381
SLCD Messages 382
SLCD-1001 382
SLCD-1002 382
SLCD-1003 382
SLCD-1004 383
SLCD-1005 383
SLCD-1006 383
SLCD-1007 383
SLCD-1008 384
SLCD-1009 384
SLCD-1010 384
SLCD-1011 385
SNMP Messages 385
SNMP-1001 385
SNMP-1002 385
SNMP-1003 385
SNMP-1004 386
SNMP-1005 386
SRM Messages 386
SRM-1001 386
SRM-1002 387
SRM-1003 387
SRM-1004 387
SRM-1005 388
SS Messages 388
SS-1000 388
SS-1001 388
SS-1002 389
SS-1003 389
SS-1004 390
SS-1010 390
SS-1011 390
SS-1012 391
SS-1013 391
SS-1014 391
SS-1015 392
SS-1016 392
SS-1017 392
SS-1018 392
SSMD Messages 393
SSMD-1001 393

SSMD-1002 393
SSMD-1003 393
SSMD-1004 393
SSMD-1005 394
SSMD-1136 394
SSMD-1236 394
SSMD-1400 395
SSMD-1402 395
SSMD-1404 395
SSMD-1405 395
SSMD-1406 396
SSMD-1407 396
SSMD-1408 396
SSMD-1409 396
SSMD-1410 397
SSMD-1411 397
SSMD-1412 397
SSMD-1413 397
SSMD-1436 398
SSMD-1437 398
SSMD-1438 398
SSMD-1439 399
SSMD-1440 399
SSMD-1498 399
SSMD-1499 399
SSMD-1536 400
SSMD-1571 400
SSMD-1900 400
SSMD-1901 400
SSMD-1902 401
SSMD-1915 401
SULB Messages 401
SULB-1000 401
SULB-1100 402
SULB-1101 402
SULB-1102 402
SULB-1103 404
SULB-1104 404
SULB-1105 406
SULB-1106 406
SULB-1107 406
SULB-1108 407
SULB-1109 407
SULB-1110 407
SULB-1211 408
SULB-1212 408
SULB-1213 409
SULB-1214 409
SWCH Messages 409

SWCH-1001 409
SWCH-1002 409
SWCH-1004 410
SWCH-1005 410
SWCH-1007 410
SWCH-1021 411
SWCH-1023 411
SWCH-1024 411
TNDL Messages 412
TNDL-1000 412
TNDL-1001 412
TNDL-1005 412
TNDL-1006 412
TNDL-1007 413
TNDL-2001 413
TNDL-2011 413
TNDL-2012 414
TNDL-2013 414
TNDL-2014 414
TNDL-2015 414
TNLD-2016 415
TNDL-2017 415
TOAM Messages 415
TOAM-1003 415
TRCE Messages 416
TRCE-1002 416
TRCE-1003 416
TRCE-1005 416
TRCE-1006 417
TRCE-1007 417
TRCE-1008 417
TRCE-1009 417
TRCE-1010 418
TRCE-1011 418
TRCE-1012 418
TS Messages 419
TS-1001 419
TS-1002 419
TS-1008 420
TS-1009 420
TS-1010 420
TS-1011 421
TS-1012 421
TS-1013 421
UCST Messages 421
UDLD Messages 422
UDLD-1000 422
UDLD-1001 422
UDLD-1002 422

UDLD-1003 422
UDLD-1004 423
UDLD-1005 423
UDLD-1006 423
UDLD-1007 423
UPTH Messages 424
UPTH-1001 424
VRRP Messages 424
VRRP-1001 424
VRRP-1002 424
VRRP-1003 425
VRRP-1004 425
VRRP-1005 425
VRRP-1006 425
VRRP-1007 426
VRRP-1008 426
VRRP-1009 426
VRRP-1010 426
VRRP-1501 427
VRRP-1502 427
VRRP-1503 427
VRRP-1504 427
VRRP-1505 428
VRRP-1506 428
VRRP-1507 428
VRRP-1508 428
VRRP-1509 429
VRRP-1510 429
VRRP-1511 429
VRRP-1512 429
VRRP-1513 429
VRRP-1514 430
VRRP-1515 430
VRRP-1516 430
VRRP-2001 430
VRRP-2002 431
VRRP-2003 431
VRRP-2004 431
VRRP-2005 431
VRRP-2006 432
VRRP-2007 432
VRRP-2008 432
VRRP-2009 432
VRRP-2010 433
VRRP-2011 433
VRRP-2012 433
VRRP-2013 433
VRRP-2014 433
VRRP-2015 434

VRRP-2016 434
VRRP-2017 434
VRRP-2018 434
VRRP-2019 435
VRRP-2020 435
VRRP-2021 435
VRRP-2022 435
VRRP-2023 436
VRRP-5001 436
VRRP-5201 436
VRRP-5301 436
VRRP-5302 436
VRRP-5303 437
VRRP-5304 437
WEBD Messages 437
WEBD-1001 437
WEBD-1002 438
WEBD-1004 438
WEBD-1005 438
WEBD-1006 438
WEBD-1007 439
WEBD-1008 439
WEBD-1009 439

Preface

Read the following topics to learn about:

- The meanings of text formats used in this document.
- Where you can find additional information and help.
- How to reach us with questions and comments.

Text Conventions

Unless otherwise noted, information in this document applies to all supported environments for the products in question. Exceptions, like command keywords associated with a specific software version, are identified in the text.

When a feature, function, or operation pertains to a specific hardware product, the product name is used. When features, functions, and operations are the same across an entire product family, such as Extreme Networks switches, the product is referred to as *the switch*.

Table 1: Notes and warnings

Icon	Notice type	Alerts you to...
	Tip	Helpful tips and notices for using the product
	Note	Useful information or instructions
	Important	Important features or instructions
	Caution	Risk of personal injury, system damage, or loss of data
	Warning	Risk of severe personal injury

Table 2: Text

Convention	Description
`screen displays`	This typeface indicates command syntax, or represents information as it is displayed on the screen.
The words *enter* and *type*	When you see the word *enter* in this guide, you must type something, and then press the Return or Enter key. Do not press the Return or Enter key when an instruction simply says *type*.
Key names	Key names are written in boldface, for example **Ctrl** or **Esc**. If you must press two or more keys simultaneously, the key names are linked with a plus sign (+). Example: Press **Ctrl**+**Alt**+**Del**
Words in italicized type	Italics emphasize a point or denote new terms at the place where they are defined in the text. Italics are also used when referring to publication titles.
NEW!	New information. In a PDF, this is searchable text.

Table 3: Command syntax

Convention	Description
bold text	Bold text indicates command names, keywords, and command options.
italic text	Italic text indicates variable content.
`[ ]`	Syntax components displayed within square brackets are optional. Default responses to system prompts are enclosed in square brackets.
`{ x | y | z }`	A choice of required parameters is enclosed in curly brackets separated by vertical bars. You must select one of the options.
`x | y`	A vertical bar separates mutually exclusive elements.
`< >`	Nonprinting characters, such as passwords, are enclosed in angle brackets.
...	Repeat the previous element, for example, *member*`[`*member*`...]`.
\	In command examples, the backslash indicates a "soft" line break. When a backslash separates two lines of a command input, enter the entire command at the prompt without the backslash.

Documentation and Training

Find Extreme Networks product information at the following locations:

Current Product Documentation
Release Notes

Hardware and Software Compatibility for Extreme Networks products
Extreme Optics Compatibility
Other Resources such as articles, white papers, and case studies

Open Source Declarations

Some software files have been licensed under certain open source licenses. Information is available on the Open Source Declaration page.

Training

Extreme Networks offers product training courses, both online and in person, as well as specialized certifications. For details, visit the Extreme Networks Training page.

Help and Support

If you require assistance, contact Extreme Networks using one of the following methods:

Extreme Portal

Search the GTAC (Global Technical Assistance Center) knowledge base; manage support cases and service contracts; download software; and obtain product licensing, training, and certifications.

The Hub

A forum for Extreme Networks customers to connect with one another, answer questions, and share ideas and feedback. This community is monitored by Extreme Networks employees, but is not intended to replace specific guidance from GTAC.

Call GTAC

For immediate support: (800) 998 2408 (toll-free in U.S. and Canada) or 1 (408) 579 2800. For the support phone number in your country, visit www.extremenetworks.com/support/contact.

Before contacting Extreme Networks for technical support, have the following information ready:

- Your Extreme Networks service contract number, or serial numbers for all involved Extreme Networks products
- A description of the failure
- A description of any actions already taken to resolve the problem
- A description of your network environment (such as layout, cable type, other relevant environmental information)
- Network load at the time of trouble (if known)
- The device history (for example, if you have returned the device before, or if this is a recurring problem)
- Any related RMA (Return Material Authorization) numbers

Subscribe to Product Announcements

You can subscribe to email notifications for product and software release announcements, Field Notices, and Vulnerability Notices.

1. Go to The Hub.
2. In the list of categories, expand the **Product Announcements** list.
3. Select a product for which you would like to receive notifications.
4. Select **Subscribe**.
5. To select additional products, return to the **Product Announcements** list and repeat steps 3 and 4.

You can modify your product selections or unsubscribe at any time.

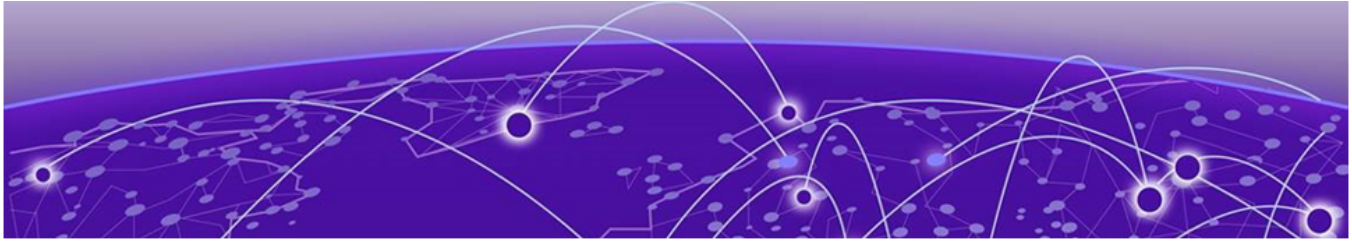
Send Feedback

The User Enablement team at Extreme Networks has made every effort to ensure that this document is accurate, complete, and easy to use. We strive to improve our documentation to help you in your work, so we want to hear from you. We welcome all feedback, but we especially want to know about:

- Content errors, or confusing or conflicting information.
- Improvements that would help you find relevant information.
- Broken links or usability issues.

To send feedback, email us at Product-Documentation@extremenetworks.com.

Provide as much detail as possible including the publication title, topic heading, and page number (if applicable), along with your comments and suggestions for improvement.



About This Document

What's New in this Document on page 36
Supported Hardware on page 36

What's New in this Document

This document is released with the SLX-OS 20.7.3 software release.

Table 4: Changes made in Rev AB of this document

Feature	Description	Described in
DCM Messages	Added the following DMC Messages: DCM-1471 DCM-1472 DCM-1473 DCM-1474 DCM-1475	DCM Messages

Rev AA of this document was released with the SLX-OS 20.7.3 software release. No changes were made to this document for this revision.

For additional information, refer to the *Extreme SLX-OS Release Notes* for this version.

Supported Hardware

For instances in which a topic or part of a topic applies to some devices but not to others, the topic specifically identifies the devices.

SLX-OS 20.7.3 supports the following hardware platforms.

- Extreme 8820
- Extreme 8720
- Extreme 8520
- ExtremeSwitching SLX 9540
- ExtremeSwitching SLX 9250
- ExtremeSwitching SLX 9150

- ExtremeRouting SLX 9740
- ExtremeRouting SLX 9640

Note

All configurations and software features that are applicable to SLX 9150 and SLX 9250 devices are also applicable for the Extreme 8520 and Extreme 8720 devices respectively.

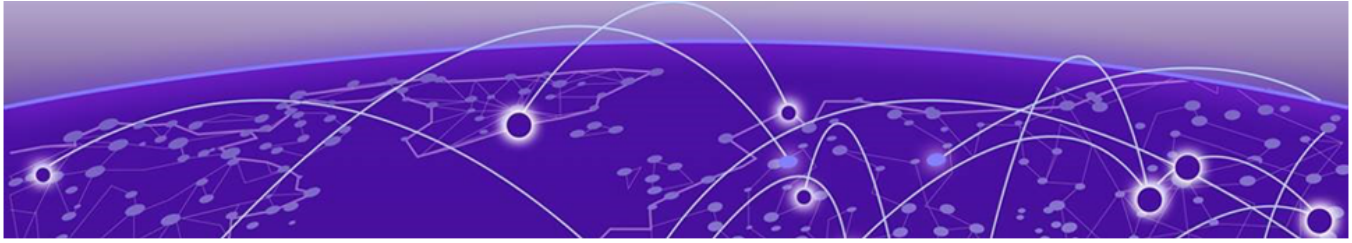
All configurations and software features that are applicable to SLX 9740 devices are also applicable for the Extreme 8820 devices.

The "Measured Boot with Remote Attestation" feature is only applicable to the Extreme 8520, Extreme 8720, and Extreme 8820 devices. It is not supported on the SLX 9150 and SLX 9250 devices.

Note

Although many software and hardware configurations are tested and supported for this release, documenting all possible configurations and scenarios is beyond this document's scope.

For information about other releases, see the documentation for those releases.



SLX-OS Messaging

Overview of RASLog messages on page 38
Configuring the syslog message destinations on page 42
Configuring the SNMP server hosts on page 45
Commands for displaying, clearing, and configuring the message logs on page 49
Displaying message content on the switch on page 50
Configuring system messages on page 51
Viewing and clearing the RASLog messages on page 52
Viewing, clearing, and configuring AUDIT log messages on page 56
Understanding RASLog messages on page 59
Responding to a RASLog message on page 62
System module descriptions on page 64

Overview of RASLog messages

Reliability, Availability and Serviceability (RAS) log messages were named RASLog messages by IBM and are used to log system events that are related to configuration changes or system error conditions. Messages are reported at various levels of severity ranging from informational (INFO) to escalating error levels (WARNING, ERROR, and CRITICAL). SLX-OS maintains two separate internal message storage repositories, SYSTEM and DCE. The following table shows the message types that are stored in each repository. A RASLog message can have one or more type attributes. For example, a message can be of type DCE, FFDC, and AUDIT. A message cannot have both LOG and DCE type attributes.

Table 5: Message type matrix

Message type	DCE message repository	SYSTEM message repository
LOG	**No**	Yes
DCE	Yes	**No**
CFFDC	Yes	Yes
FFDC	Yes	Yes
AUDIT	Yes	Yes

RASLog message types

SLX-OS supports different types of RASLog messages. The following sections describe in detail the message types.

1. System messages: System or LOG messages report significant system-level events or information and are also used to show the status of the high-level, user-initiated actions. System messages are stored in a separate nonvolatile storage and are preserved across the firmware upgrade or downgrade. The system messages are forwarded to the console, to the configured syslog servers, and through the SNMP traps or informs to the SNMP management station.

   The following example shows a system message.

   ```
   2017/09/14-23:26:44, [FW-1424], 620, M1 | Active, WARNING, SLX9850-8, Switch status
   changed from HEALTHY to MARGINAL.
   ```

   For information on displaying and clearing the system messages, refer to Viewing and clearing the RASLog messages.
2. DCE RASLog messages: DCE RASLog messages report error-related events and information in the protocol-based modules such as network service module (NSM), system services manager (SSM), and so on. DCE messages are stored in a separate nonvolatile storage and are preserved across the firmware upgrades. The DCE messages are forwarded to the console, to the configured syslog servers, and through the SNMP traps or informs to the SNMP management station.

   The following example shows a DCE message.

   ```
   2017/09/14-23:26:25, [NSM-1004], 617, M1 | Active | DCE, INFO, SLX9850-8,  Vlan 1 is
   created.
   ```

   For information on displaying and clearing the DCE RASLog messages, refer to Viewing and clearing the RASLog messages
3. AUDIT log messages: Event auditing is designed to support post-event audits and problem determination that are based on high-frequency events of certain types, such as security violations, firmware downloads, and configuration. AUDIT log messages are saved in the persistent storage. The storage has a limit of 1024 entries and wraps around if the number of messages exceeds the limit. The switch can be configured to stream AUDIT messages to the specified syslog servers. The AUDIT log messages are not forwarded to an SNMP management station.

   The following example shows an AUDIT log message.

   ```
   891 AUDIT, 2017/09/14-23:30:29 (GMT), [SEC-3024], INFO, SECURITY, NONE/root/NONE/None/
   CLI,, SLX9850-8, Event: passwd, Status: success, Info: User account [user], password
   changed.
   ```

   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 root or admin.
- Event Name: The name of the event that occurred.
- Status: The status of the event that occurred: success or failure.
- Event Info: Information about the event.

The following table describes the three event classes that can be audited.

Table 6: Event classes of the AUDIT messages

Event class	Operand	Description
DCMCFG	CONFIGURATION	You can audit all the configuration changes in the OS.
FIRMWARE	FIRMWARE	You can audit the events occurring during the firmware download process.
SECURITY	SECURITY	You can audit any user-initiated security event for all management interfaces. For events that have an impact on the entire network, an audit is generated only for the switch from which the event was initiated.

You can enable event auditing by configuring the syslog daemon to send the events to a configured remote host by using the **`logging syslog-server`** command. You can set up filters to screen out particular classes of events by using the **`logging auditlog class`** command (the classes include SECURITY, CONFIGURATION, and FIRMWARE). All the AUDIT classes are enabled by default. The defined set of AUDIT messages are 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, refer to Viewing, clearing, and configuring AUDIT log messages.

4. FFDC messages: First Failure Data Capture (FFDC) is used to capture failure-specific data when a problem or failure is first noted and before the switch reloads or the trace and log buffer get wrapped. All subsequent iterations of the same error are ignored. This critical debug information is saved in nonvolatile storage and can be retrieved by entering the **`copy support`** command. The data are used for debugging purposes. FFDC is intended for use by Extreme Networks technical support. FFDC is enabled by default. Enter the **`support`** command to enable or disable FFDC. If FFDC is disabled, the FFDC daemon does not capture any data, even when a message with FFDC attributes is logged.

   The following example shows an FFDC message.

```
2017/09/14-23:28:18, [HASM-1200], 666, L1/0 | Active | FFDC, WARNING, SLX9850-8,
Detected termination of process hslagtd:2915.
```

You can display the FFDC messages by using the **show logging raslog attribute FFDC** command. For information on displaying the FFDC RASLog messages, refer to Viewing and clearing the RASLog messages.

5. CFFDC messages: Chassis-wide FFDC (CFFDC) is used to capture FFDC data for every management module (MM) or line card (LC) in the entire chassis for failure analysis. This debug information is saved in nonvolatile storage and can be retrieved by entering the **copy support** command. If FFDC is disabled, the CFFDC data is not captured even when a message with the CFFDC attribute is logged.

   The following example shows a CFFDC message.

```
2017/10/14-10:36:51, [EM-1100], 28749, M2 | Active | CFFDC, CRITICAL, SLX9850-8, Unit
in L3 with ID 127 is faulted(119). 1 of 1 total attempt(s) at auto-recovery is being
made. Delay is 60 seconds.
```

Message severity levels

Messages have four levels of severity, ranging from CRITICAL to INFO. In general, the definitions are wide ranging and are to be used as general guidelines for troubleshooting. In all cases, you must look at each specific error message description thoroughly before taking action. The following table lists the RASLog message severity levels.

Table 7: Severity levels of the RASLog messages

Severity level	Description
CRITICAL	A CRITICAL message indicates that the software has detected serious problems that cause a partial or complete failure of a subsystem if not corrected immediately; for example, a power supply failure or rise in temperature must receive immediate attention.
ERROR	An ERROR message represents an error condition that does not affect overall system functionality significantly. For example, an ERROR message may indicate a timeout on a certain operation, a failure of a certain operation after a retry, an invalid parameter, or a failure to perform a requested operation.
WARNING	A WARNING message highlights a current operating condition that must 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.
INFO	An INFO message reports the current nonerror status of the system components; for example, detecting online and offline status of an interface.

RASLog message logging

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

- SYSTEM and DCE messages are saved to separate nonvolatile storage repositories.
- SYSTEM and DCE message logs can save a maximum of 4096 messages.

- The message log is implemented as a circular buffer. When more than the maximum entries are added to the log file, new entries overwrite old entries.
- Messages are numbered sequentially from 1 through 2,147,483,647 (0x7fffffff). The sequence number continues to increase after the message log wraps around. The message sequence numbering is not split for the system and DCE message logs. The sequence number can be reset to 1 by using the **clear logging raslog** command. However, the sequence number is not reset to 1 if you clear a particular message type, for example, DCE.
- Trace dump, FFDC, and core dump files can be uploaded to the FTP server by using the **copy support ftp** command.

Extreme Networks recommends that you configure the system logging daemon (syslogd) facility as a management tool for error logs. For more information, refer to Configuring the syslog message destinations.

Configuring the syslog message destinations

You can configure a switch to send the syslog messages to the following output locations: syslog daemon, system console, and 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. The 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 the standard syslogd functionality. All the RASLog messages are forwarded to the syslogd. Configuring for syslogd involves configuring the host, enabling syslogd on the Extreme Networks model, and optionally, setting the facility level.

Configuring a syslog server: To configure the switch to forward all RASLog messages to the syslogd of one or more servers, perform the following steps.

1. Enter the **configure terminal** command to access the global configuration level of the CLI.

```
device# configure terminal
Entering configuration mode terminal
```

2. Enter the **logging syslog-server** IP address command to add a server to which the messages are forwarded. You can configure a syslog server in IPv4 or IPv6 format. The following example shows how to configure a syslog server with an IPv4 address.

```
device(config)# logging syslog-server 192.0.2.2
```

   You can configure as many as four syslog servers to receive the syslog messages.
3. Enter the **format** command to configure the syslog server to use the RFC-5424 format for messages.

```
device(config-syslog-server-192.0.2.2)# format RFC-5424
```

The following example shows a SEC-3022 message in the format before configuring the syslog server to use the RFC-5424 format for messages:

```
<190>Nov 30 01:00:03 SLX8-1 raslogd: [log@1588 value="RASLOG"][msgid@1588
value="SEC-3022"][seqnum@1588 value="6681"][attr@1588 value=" M1 | Active | WWN
10:00:c4:f5:7c:50:01:16"][severity@1588 value="INFO"][swname@1588 value="SLX9850-8"]
[arg0@1588 value="logout" desc="Event Name"][arg1@1588 value="admin" desc="User"]
BOMEvent: logout, Status: success, Info: Successful logout by user [admin].
```

The following example shows a SEC-3022 message in the format after configuring the syslog server to use the RFC-5424 format for messages:

```
<190>1 2017-11-30T01:00:03+00:00 SLX8-1 raslogd - - [meta sequenceId="2"][log@1588
value="RASLOG"][msgid@1588 value="SEC-3022"][seqnum@1588 value="6681"][attr@1588
value=" M1 | Active | WWN 10:00:c4:f5:7c:50:01:16"][severity@1588 value="INFO"]
[swname@1588 value="SLX9850-8"][arg0@1588 value="logout" desc="Event Name"][arg1@1588
value="admin" desc="User"] BOMEvent: logout, Status: success, Info: Successful logout
by user [admin].
```

4. Enter the **show running-config logging syslog-server** command to verify the syslog configuration on the switch.

```
device# show running-config logging syslog-server
logging syslog-server 192.0.2.2
 format RFC-5424
```

The following example shows how to configure a syslog server with an IPv6 address.

```
device# configure terminal
Entering configuration mode terminal
device(config)# logging syslog-server 2017:DB8::32
device(config)# exit
device# show running-config logging syslog-server
logging syslog-server 2017:db8::32
```

You can remove a configured syslog server by using the **no logging syslog-server IP address** command.

Setting the syslog facility: The syslog facility is a configurable parameter that specifies the log file to which messages are forwarded. You must configure the syslog servers to receive system messages before you can configure the syslog facility. To set the syslog facility, perform the following steps.

1. Enter the **configure terminal** command to access the global configuration level of the CLI.

```
device# configure terminal
Entering configuration mode terminal
```

2. Enter the **logging syslog-facility local** *log_level* command to set the syslog facility to a specific log file.

   The *log_level* argument specifies the syslog facility and can be a value from LOG_LOCAL0 through LOG_LOCAL7. The default syslog level is LOG_LOCAL7. The following example show how to set the syslog facility level to LOG_LOCAL2.

```
device(config)# logging syslog-facility local LOG_LOCAL2
```

3. Enter the **show running-config logging syslog-facility** command to verify the syslog facility configuration on the switch.

```
device# show running-config logging syslog-facility
logging syslog-facility local LOG_LOCAL2
```

You can reset the syslog facility to the default (LOG_LOCAL7) by using the **no logging syslog-facility local** command.

System console

The system console displays all RASLog messages, AUDIT messages (if enabled), and panic dump messages. These messages are mirrored to the system console; they are always saved in one of the message 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 do not receive system console messages.

You can filter messages by severity that are displayed on the system console by using the **logging raslog console** command. All messages are still sent to the system message log, syslog (if enabled), and SNMP management station.

You can use the **logging raslog console** [**stop** [*minutes*] | **start**] command to disable and re-enable the RASLog messages from being displayed on the system console.

Setting the RASLog console severity level: You can limit the types of messages that are logged to the console by using the **logging raslog console** command. The RASLog messages that are displayed on the console are passed up to and above the configured severity level. For example, if you configure the console severity level to ERROR, only ERROR and CRITICAL messages pass through. You can choose one of the following severity levels: INFO, WARNING, ERROR, or CRITICAL.The default severity level is INFO.

To set the severity levels for the RASLog console, perform the following step.

1. Enter the **configure terminal** command to access the global configuration level of the CLI.

```
device# configure terminal
Entering configuration mode terminal
```

SNMP management station

When an unusual event, an error, or a status change occurs on the device, an event notification is sent to the SNMP management station. Network OS v7.1.0 supports two types of event notifications: traps (in SNMPv1, SNMPv2c, and SNMPv3) and informs (in SNMPv3).

1. SNMP traps: 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, 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 possible severity levels follow:

- Critical
- Debug
- Error
- Info
- None
- Warning

By default, the severity level is set to None, implying all traps are filtered and, therefore, no event traps are received. When the severity level is set to Info, all traps with the severity level of Info, Warning, Error, and Critical are received.

Note
The AUDIT log messages are not converted into swEventTrap.

The 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.

Extreme Networks switches send traps out on UDP port 162. To receive traps, the management station IP address must be configured on the switch. You can configure the SNMPv1, SNMPv2c, and SNMPv3 hosts to receive the traps. For more information, refer to "Configuring the SNMP (version 1 or version 2c) server host" Configuring the SNMP server hosts.

2. SNMP informs: An SNMP inform is similar to the SNMP trap except that the management station that receives an SNMP inform acknowledges the system message with an SNMP response PDU. If the sender does not receive the SNMP response, the SNMP 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. The SNMP informs are more reliable and they consume more resources in the device and in the network. Use SNMP informs only if it is important that the management station receives all event notifications. Otherwise, use the SNMP traps.

   Extreme Networks devices support SNMPv3 informs. For more information, refer to "Configuring the SNMPv3 server" Configuring the SNMP server hosts.

Configuring the SNMP server hosts

SLX-OS supports SNMP version 1, version 2c, and version 3. Use the commands listed in the following table to configure the SNMPv1, SNMPv2c, and SNMPv3 hosts and their configurations.

Table 8: Commands for configuring SNMP server hosts

Command	Description
[**no**] **snmp-server host** {*ipv4-host* | *ipv6-host* | *dns-host*} *community-string* [**severity-level** [**none** | **debug** | **info** | **warning** | **error** | **critical**] [**udp-port** *port_number*] [**version** [**1** | **2c**]	This command sets the destination IP addresses, version, community string (for version 1 and version 2c), and destination port for the traps. The **severity-level** option is used to filter the traps based on severity. The **no** form of the command changes the SNMP server host configurations to the default value.
[**no**] **snmp-server v3host** {*ipv4-host* | *ipv6-host* | *dns-host*} *username* [**notifytype** {**traps** | **informs**}] **engineid** *engine-id* **severity-level** [**none** | **debug** | **info** | **warning** | **error** | **critical**] **udp-port** *port_number*	This command specifies the recipient of the SNMP version 3 notification option. The **severity-level** option is used to filter the traps or informs based on severity. Use the **no** form of the command to remove a specific host.

Configuring the SNMP (version 1 or version 2c) server host

To set the trap destination IP addresses, version (1 or 2c), community string for SNMP version 1 and version 2c, and the destination port for the SNMP traps, perform the following steps.

1. Enter the **configure terminal** command to access the global configuration level of the CLI.

```
device# configure terminal
Entering configuration mode terminal
```

2. Enter the following command to set the trap recipient with IP address 192.0.2.2, which receives all traps with the severity levels of Critical, Error, Info, and Warning.

```
device(config)# snmp-server host 192.0.2.2 public severity-level Info udp-port
162 version 1
```



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

3. Enter the **do show running-config snmp-server** command to verify the configuration.

```
device(config)# do show running-config snmp-server
snmp-server sys-descr "Extreme SLX9740-80C Switch/Router"
snmp-server engineID local 80:0:6:34:b2:7e:88:0:10:a:14:d3:25
snmp-server community $9$5NQFNEVN67kKklzWw+b/rg== groupname group2
snmp-server community $9$dlGJTAP4O2fz40uz+6p24g== groupname group1
snmp-server community $9$ZqrZyV4ln8u5MqJeUGHblg== groupname group3
snmp-server host 10.20.192.72 $9$5NQFNEVN67kKklzWw+b/rg==
 version 2c
 severity-level Info
!
snmp-server host 10.20.192.72 $9$dlGJTAP4O2fz40uz+6p24g==
```

```
 severity-level Info
!
snmp-server user snmpteam1 groupname group3 auth sha auth-password nHW0ev6kLY priv
AES128 priv-password nHW0ev6kLY encrypted
snmp-server user snmpteam3 groupname group3 auth md5 auth-password XoooIwNn47 priv
AES128 priv-password XoooIwNn47 encrypted
snmp-server user snmpteam4 groupname grpauth_nopriv auth sha auth-password nHW0ev6kLY
encrypted
snmp-server user user groupname group3 auth md5 auth-password XoooIwNn47 priv AES128
priv-password XoooIwNn47 encrypted
snmp-server v3host 10.20.192.72 snmpteam1
 severity-level Info
!
snmp-server view all 1 included
snmp-server view All 1 included
snmp-server group group1 v1 read all write all notify all
snmp-server group group2 v2c read all write all notify all
snmp-server group group3 v3 priv read all write all notify all
snmp-server group grpauth_nopriv v3 auth read All write All notify All
dutA(config)# do show running-config snmp-server
snmp-server sys-descr "Extreme SLX9740-80C Switch/Router"
snmp-server engineID local 80:0:6:34:b2:7e:88:0:10:a:14:d3:25
snmp-server community $9$5NQFNEVN67kKklzWw+b== groupname group2
snmp-server community $9$dlGJTAP4O2fz40uz+6p== groupname group1
snmp-server community $9$ZqrZyV4ln8u5MqJeUGH== groupname group3
snmp-server host 10.20.192.72 $9$5NQFNEVN67kKklzWw+b==
 version 2c
 severity-level Info
!
snmp-server host 10.20.192.72 $9$dlGJTAP4O2fz40uz+6p==
 severity-level Info
!
snmp-server user snmpteam1 groupname group3 auth sha auth-password nHW0ev6kLY priv
AES128 priv-password nHW0ev6kLY encrypted
snmp-server user snmpteam3 groupname group3 auth md5 auth-password XoooIwNn47 priv
AES128 priv-password XoooIwNn47 encrypted
snmp-server user snmpteam4 groupname grpauth_nopriv auth sha auth-password nHW0ev6kLY
encrypted
snmp-server user user groupname group3 auth md5 auth-password XoooIwNn47 priv AES128
priv-password XoooIwNn47 encrypted
snmp-server v3host 10.20.192.72 snmpteam1
 severity-level Info
!
snmp-server view all 1 included
snmp-server view All 1 included
snmp-server group group1 v1 read all write all notify all
snmp-server group group2 v2c read all write all notify all
snmp-server group group3 v3 priv read all write all notify all
snmp-server group grpauth_nopriv v3 auth read All write All notify All
device(config)#
```

Configuring the SNMPv3 server

Use the **snmp-server v3-host** command to specify the recipient of SNMP version 3 notifications: traps or informs. The following example describes the procedure for configuring the recipient of the SNMPv3 informs.

To configure the SNMPv3 host to receive the inform, perform the following steps.

1. Enter the **configure terminal** command to access the global configuration level of the CLI.

```
device# configure terminal
Entering configuration mode terminal
```

2. Enter the following command to set the inform recipient with IP address 192.0.2.2, which receives all traps with the severity levels of Critical, Error, Info, and Warning.

```
device(config)# snmp-server v3host 192.0.2.2 snmpadmin1 notifytype informs
engineid 80:00:05:23:01:AC:1A:01:79 severity-level Info udp-port 4425
```



Note

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

3. Enter the **show running-config snmp-server** command to verify the configuration.

```
device(config)# do show running-config snmp-server
snmp-server sys-descr "Extreme SLX9740-80C Switch/Router"
snmp-server engineID local 80:0:6:34:b2:7e:88:0:10:a:14:d3:25
snmp-server community $9$5NQFNEVN67kKklzWw+b/rg== groupname group2
snmp-server community $9$dlGJTAP4O2fz40uz+6p24g== groupname group1
snmp-server community $9$ZqrZyV4ln8u5MqJeUGHblg== groupname group3
snmp-server host 10.20.192.72 $9$5NQFNEVN67kKklzWw+b/rg==
 version 2c
 severity-level Info
!
snmp-server host 10.20.192.72 $9$dlGJTAP4O2fz40uz+6p24g==
 severity-level Info
!
snmp-server user snmpteam1 groupname group3 auth sha auth-password nHW0ev6kLY priv
AES128 priv-password nHW0ev6kLY encrypted
snmp-server user snmpteam3 groupname group3 auth md5 auth-password XoooIwNn47 priv
AES128 priv-password XoooIwNn47 encrypted
snmp-server user snmpteam4 groupname grpauth_nopriv auth sha auth-password nHW0ev6kLY
encrypted
snmp-server user user groupname group3 auth md5 auth-password XoooIwNn47 priv AES128
priv-password XoooIwNn47 encrypted
snmp-server v3host 10.20.192.72 snmpteam1
 severity-level Info
!
snmp-server view all 1 included
snmp-server view All 1 included
snmp-server group group1 v1 read all write all notify all
snmp-server group group2 v2c read all write all notify all
snmp-server group group3 v3 priv read all write all notify all
snmp-server group grpauth_nopriv v3 auth read All write All notify All
dutA(config)# do show running-config snmp-server
snmp-server sys-descr "Extreme SLX9740-80C Switch/Router"
snmp-server engineID local 80:0:6:34:b2:7e:88:0:10:a:14:d3:25
snmp-server community $9$5NQFNEVN67kKklzWw+b== groupname group2
snmp-server community $9$dlGJTAP4O2fz40uz+6p== groupname group1
snmp-server community $9$ZqrZyV4ln8u5MqJeUGH== groupname group3
snmp-server host 10.20.192.72 $9$5NQFNEVN67kKklzWw+b==
 version 2c
 severity-level Info
!
snmp-server host 10.20.192.72 $9$dlGJTAP4O2fz40uz+6p==
 severity-level Info
!
```

```
snmp-server user snmpteam1 groupname group3 auth sha auth-password nHW0ev6kLY priv
AES128 priv-password nHW0ev6kLY encrypted
snmp-server user snmpteam3 groupname group3 auth md5 auth-password XoooIwNn47 priv
AES128 priv-password XoooIwNn47 encrypted
snmp-server user snmpteam4 groupname grpauth_nopriv auth sha auth-password nHW0ev6kLY
encrypted
snmp-server user user groupname group3 auth md5 auth-password XoooIwNn47 priv AES128
priv-password XoooIwNn47 encrypted
snmp-server v3host 10.20.192.72 snmpteam1
 severity-level Info
!
snmp-server view all 1 included
snmp-server view All 1 included
snmp-server group group1 v1 read all write all notify all
snmp-server group group2 v2c read all write all notify all
snmp-server group group3 v3 priv read all write all notify all
snmp-server group grpauth_nopriv v3 auth read All write All notify All
device(config)#
```

Commands for displaying, clearing, and configuring the message logs

The following table describes commands that you can use to view or configure various message logs. Most commands require the admin access level. For detailed information on required access levels and commands, refer to *Extreme SLX-OS Command Reference*.

Table 9: Commands for viewing and configuring the message logs

Command	Description
clear logging auditlog	Clears the AUDiT log messages from the local switch or the specific switches.
clear logging raslog	Sets a filter that is based on the severity level for the messages to be displayed on the system console.
logging auditlog class	Sets the event classes for AUDIT log messages.
logging raslog console	Sets a filter that is based on the severity level for the messages to be displayed on the system console.
logging syslog-facility local	Sets the syslog facility.
logging syslog-server	Configures a syslog server to which the switch can forward the messages.
format RFC-5424	Configures a syslog server to RFC-5424 format. This command is a **logging syslog-server** subcommand
show logging auditlog	Displays the AUDIT log messages on the local switch or the specific switches. **Note:** This command can be disruptive because it displays all the logs in the buffer continuously. Use **| more** to see output page by page.

Table 9: Commands for viewing and configuring the message logs (continued)

Command	Description
show logging raslog	Displays the error log message on the local switch, the specific switch, or interface module. The command includes options to filter the messages that are based on the message attribute and severity level, and also to set the count of messages to display, and to display messages in reverse order. **Note:** This command can be disruptive because it displays all the logs in the buffer continuously. Use **| more** to see output page by page.
show running-config logging	Displays the logging settings on the local switch.
show running-config logging auditlog class	Displays the event class that is configured for the AUDIT log.
show running-config logging raslog	Displays the RASLog console severity level on the local switch or the specific switch.
show running-config logging syslog-facility	Displays the syslog facility level.

Displaying message content on the switch

This section provides information on the RASLog message format.

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** *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** *message_ID* command to display the documentation of a message. The *message_ID* values are case-sensitive.

   For example, enter the following command to display the documentation for EM-1059.

```
device# rasman message id EM-1059
Miscellaneous                                    EM-1059(7m)
MESSAGE
EM-1059 - <slot number or Switch> with ID <Blade Id> may not
be supported on this platform, check firmware version as
a possible cause.

MESSAGE TYPE
   LOG

SEVERITY
   ERROR

PROBABLE CAUSE
Indicates that a a blade inserted in the specified slot or
```

```
the switch (for non-bladed switches) is incompatible with
the switch configuration software. The blade will not be
completely usable.
The blade may only be supported by a later (or earlier) version
of the firmware.

RECOMMENDED ACTION
   Change the control processor (CP) firmware or replace the
blade. Make sure the replacement is compatible with your
switch type and firmware.
```

Configuring system messages

This section provides information on configuring the system message logs.

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:

   • Enter the **logging raslog message** *message_ID* **suppress** command to disable a RASLog message. For example, enter the following command to disable the NSM-1001 message:

   ```
   switch:admin> logging raslog message NSM-1001 suppress
   2017/07/20-13:28:37, [LOG-1007], 375, M1, INFO, switch, Log message
   NS-1001 RASLOG message has been disabled.
   ```

   Use the **show running-config logging raslog message** *message_ID* command to verify the status of the message.

   • Enter the **logging raslog module** *module_ID* command to disable all messages in a module. For example, enter the following command to disable all messages that belong to the NSM module:

   ```
   switch:admin> logging raslog module NSM
   2017/07/20-13:28:37, [LOG-1007], 375, CHASSIS, INFO, switch, Log Module
   NSM module RASLOG message has been suppress.
   ```

   Use the **show running-config logging raslog module** *module_ID* command to verify the status of the messages that belong to a module.

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:

• Enter the **no logging raslog message** *message_ID* **suppress** command to enable a single RASLog message that has been disabled. For example, enter the following command to enable the NSM-1001 message that was previously disabled:

```
switch:admin> no logging raslog message NS-1001 suppress
2017/07/20-13:24:43, [LOG-1008], 374, M1, INFO, switch, Log Module NSM-1001
RASLOG message has been enabled.
```

Use the **show running-config logging raslog message** *message_ID* command to verify the status of the message.

• Enter the **no logging raslog module** *module_ID* command to enable all messages in a module. For example, enter the following command to enable to all previously disabled NSM messages:

```
switch:admin> no logging raslog module NSM
2017/07/20-13:24:43, [LOG-1008], 374, M1, INFO, switch, Log Module NSM has
been enabled.
```

Use the **show running-config logging raslog 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 **logging raslog message** *message_ID* **severity** [**CRITICAL** | **ERROR** | **WARNING** | **INFO**] command to change the severity level of a message. For example, enter the following command to change the severity level of the SEC-1203 message to WARNING.

```
switch:admin> logging raslog message SEC-1203 severity WARNING
```

3. Use the **show running-config logging raslog message** *message_ID* severity command to verify the severity of the message.

```
switch:admin> show running-config logging raslog message SEC-1203 severity
WARNING
```

Viewing and clearing the RASLog messages

You can display the system message log by using the **show logging raslog** command. This command provides options to filter the messages by attribute, message type, severity, or message count. You can also specify that messages be displayed for a single module by using the **blade** option. Use the **clear logging raslog** command to delete the system messages.

Displaying the RASLog messages

To display the saved RASLog messages, perform the following steps.

1. Log in to the switch as admin.
2. Enter the **show logging raslog** command at the command line.

```
device# show logging raslog
SLX: 20.5.2slxos20.5.2_230708_1000
2023/04/26-00:05:57, [LOG-1003], 1,, INFO, SLX9740-80C, SYSTEM error log has been
```

```
cleared.
2023/04/26-00:05:57, [LOG-1007], 2, DCE, INFO, SLX9740-80C, DCE error log has been
cleared.
2023/04/26-00:15:51, [SEC-3022], 3,, INFO, SLX9740-80C, Event: logout, Status:
success, Info: Successful logout by user [admin].
2023/04/27-00:00:02, [SEC-3136], 4,, WARNING, device, Event: cert expiry , Alert-
level:INFO, Certificate Details=[subject= /C=IN/ST=CHENNAI/L=Madras/O=Extreme/OU=HCL/
CN=10.20.55.129 issuer= /C=IN/ST=CHENNAI/L=Madras/O=Extreme/OU=HCL/CN=Extreme Root CA/
emailAddress=abalan@extreme.com serial=1000] will expire in 22 days.
2023/04/27-02:32:59, [SEC-1206], 5,, INFO, SLX9740-80C, Login information: User [admin
via telnet] Last Successful Login Time : Sat May  4 16:15:42 2023.
2023/04/27-02:32:59, [SEC-1203], 6,, INFO, SLX9740-80C, Login information: User
[admin] Login successful via TELNET/SSH/RSH. IP Addr: 134.141.245.254.
2023/04/27-02:48:30, [SEC-3022], 7,, INFO, SLX9740-80C, Event: logout, Status:
success, Info: Successful logout by user [admin].
2023/04/27-02:48:40, [SEC-1206], 8,, INFO, SLX9740-80C, Login information: User [admin
via telnet] Last Successful Login Time : Sat Apr 27 02:32:59 2023.
2023/04/27-02:48:40, [SEC-1203], 9,, INFO, SLX9740-80C, Login information: User
[admin] Login successful via TELNET/SSH/RSH. IP Addr: 134.141.245.254.
```

Displaying the messages on an interface module

To display the saved messages for a specific interface module, line card (LC), or management module, perform the following steps.

1. Log in to the switch as admin.
2. Enter the **`show logging raslog blade`** command at the command line. You can filter messages that are based on the severity level by using the **`severity`** option. The following example shows how to filter messages by the severity level of info.

```
device# show logging raslog blade LC2 severity info
SLX: 17r.2.00
2023/06/22-17:47:46, [HASM-1004], 52,  INFO, SLX9740-80C, Processor reloaded - Reset.
2023/06/22-17:47:46, [HASM-1104], 53,  INFO, SLX9740-80C, Heartbeat to M1 up.
2023/06/22-17:47:52, [HSL-1027], 57, L2/0 | Active, INFO, SLX-WESCON-R1,  Packet
buffers initialized (6G)
2023/06/22-17:51:02, [HASM-1108], 93, L2/0 | Active, INFO, SLX9740-80C, All service
instances become active.
2023/06/22-17:51:02, [HASM-1134], 94, L2/0 | Active, INFO, SLX9740-80C, All service
instances on Active.
2023/06/22-18:03:45, [RAS-1001], 184, L2/0 | Active, INFO, SLX9740-80C, First failure
data capture (FFDC) event occurred.
2023/06/22-18:39:43, [HASM-1004], 298, L2/0 | Standby, INFO, SLX9740-80C, Processor
reloaded - Reset.
2023/06/22-18:39:43, [HASM-1104], 299, L2/0 | Standby, INFO, SLX9740-80C, Heartbeat to
M1 up.
2023/06/22-18:39:51, [HSL-1027], 305, L2/0 | Active, INFO, SLX-WESCON-R1,  Packet
buffers initialized (6G)
2023/06/22-18:43:01, [HASM-1108], 339, L2/0 | Active, INFO, SLX9740-80C, All service
instances become active.
2023/06/22-18:43:01, [HASM-1134], 340, L2/0 | Active, INFO, SLX9740-80C, All service
instances on Active.
2023/06/22-18:45:42, [RAS-1001], 407, L2/0 | Active, INFO, SLX9740-80C, First failure
data capture (FFDC) event occurred.
2023/09/14-23:27:32, [HASM-1004], 648,  INFO, SLX9740-80C, Processor reloaded -
Reset,  HW reset reason : Plt Reset.
2023/09/14-23:27:32, [HASM-1104], 649,  INFO, SLX9740-80C, Heartbeat to M1 up.
2023/09/14-23:27:43, [HSL-1027], 657, L2/0 | Active, INFO, SLX-F8-Hamza-VS,  Packet
buffers initialized (6G)
2023/09/14-23:30:21, [HASM-1108], 720, L2/0 | Active, INFO, SLX9740-80C, All service
instances become active.
```

```
2023/09/14-23:30:21, [HASM-1134], 721, L2/0 | Active, INFO, SLX9740-80C, All service
instances on Active.
[...]
```

Clearing the RASLog messages

To clear the RASLog messages for a particular switch instance, perform the following steps.

1. Log in to the switch as admin.
2. Enter the **clear logging raslog** command to clear all messages from the switch.

Viewing and clearing the SYSTEM messages

This section provides information on viewing and clearing the SYSTEM messages saved on the switch memory.

Displaying the SYSTEM messages: To display the messages that are saved in the SYSTEM storage repository, perform the following steps.

1. Log in to the switch as admin.
2. Enter the **show logging raslog message-type SYSTEM** command at the command line.

```
device# show logging raslog message-type SYSTEM
SLX: 20.5.2
2024/04/26-00:05:57, [LOG-1003], 1,, INFO, SLX9740-80C, SYSTEM error log has been
cleared.
2024/04/26-00:15:51, [SEC-3022], 3,, INFO, SLX9740-80C, Event: logout, Status:
success, Info: Successful logout by user [admin].
2024/04/27-00:00:02, [SEC-3136], 4,, WARNING, dutA, Event: cert expiry , Alert-
level:INFO, Certificate Details=[subject= /C=IN/ST=CHENNAI/L=Madras/O=Extreme/OU=HCL/
CN=10.20.55.129 issuer= /C=IN/ST=CHENNAI/L=Madras/O=Extreme/OU=HCL/CN=Extreme Root CA/
emailAddress=abalan@extreme.com serial=1000] will expire in 22 days.
2024/04/27-02:32:59, [SEC-1206], 5,, INFO, SLX9740-80C, Login information: User [admin
via telnet] Last Successful Login Time : Sat May  4 16:15:42 2024.
2024/04/27-02:32:59, [SEC-1203], 6,, INFO, SLX9740-80C, Login information: User
[admin] Login successful via TELNET/SSH/RSH. IP Addr: 134.141.245.254.
2024/04/27-02:48:30, [SEC-3022], 7,, INFO, SLX9740-80C, Event: logout, Status:
success, Info: Successful logout by user [admin].
2024/04/27-02:48:40, [SEC-1206], 8,, INFO, SLX9740-80C, Login information: User [admin
via telnet] Last Successful Login Time : Sat Apr 27 02:32:59 2024.
2024/04/27-02:48:40, [SEC-1203], 9,, INFO, SLX9740-80C, Login information: User
[admin] Login successful via TELNET/SSH/RSH. IP Addr: 134.141.245.254.
```

Clearing the SYSTEM messages: To clear the messages that are saved in the SYSTEM storage repository, perform the following steps.

1. Log in to the switch as admin.
2. Enter the **clear logging raslog message-type SYSTEM** command to clear all system messages from the local switch.

Viewing and clearing the DCE messages

This section provides information on viewing and clearing the DCE messages that are saved in the switch memory.

Displaying the DCE messages: To display the saved DCE messages, perform the following steps.

1. Log in to the switch as admin.
2. Enter the **show logging raslog message-type DCE** command at the command line.

```
device# show logging raslog message-type DCE
SLX: 20.5.2slxos20.5.2_230708_1000
2024/04/26-00:05:57, [LOG-1007], 2, DCE, INFO, SLX9740-80C, DCE error log has been
cleared.
```

Clearing the DCE messages: To clear the DCE messages for a particular switch instance, perform the following steps.

1. Log in to the switch as admin.
2. Enter the **clear logging raslog message-type DCE** command to clear all DCE messages from the local switch.

Displaying the FFDC messages

This section provides information on viewing the FFDC messages that are saved in the switch memory.

To display the saved FFDC messages, perform the following steps.

1. Log in to the switch as admin.
2. Enter the **show logging raslog attribute FFDC** command at the command line.

```
device# show logging raslog attribute FFDC
SLX: 20.5.2
2023/06/22-17:53:07, [HASM-1200], 150, M1 | Active | FFDC, WARNING, SLX9740-80C,
Detected termination of process mpls_main:5834.
2023/09/14-23:28:18, [HASM-1200], 666, L1/0 | Active | FFDC, WARNING, SLX9740-80C,
Detected termination of process hslagtd:2915.
```

Displaying the description of the RASLog modules

To display the description of the RASLog modules, perform the following steps.

1. Log in to the switch as admin.
2. Enter the **rasman description** command at the command line.

```
device# rasman description
RASModule ID Description
-----------------------------------------------------
KT         1  Kernel Test ID
UT         2  User Test ID
TRCE       3  Trace Subsystem (User)
KTRC       4  Trace Subsystem (Kernel)
LOG        5  RASLOG module
CDR        6  Condor ASIC driver
[...]
```

Displaying RASLog messages in a module

To display the list of all RASLog messages in a module with their message text, perform the following steps.

1. Log in to the switch as admin.
2. Enter the **rasman module name** *module_name* command at the command line. For example, enter the following command to display all messages in the AUTH module.

```
device# rasman module name AUTH
RAS Message        ID            Severity Message
-------------------------------------------------------------------------------------------
--------
AUTH-1001          INFO          %s has been successfully completed.
AUTH-1002          ERROR          %s has failed.
AUTH-1003          INFO          %s type has been successfully set to %s.
AUTH-1004          ERROR          Failed to set %s type to %s.
AUTH-1005          ERROR          Authentication file does not exist: %d.
AUTH-1006          WARNING      Failed to open authentication configuration file.
AUTH-1007          ERROR          The proposed authentication protocol(s) are not
supported: port %d.
AUTH-1008          ERROR          No security license, operation failed.
[...]
```

Displaying RASLog messages by type: To display the list of RASLog messages that are based on the message type, perform the following steps.

1. Log in to the switch as admin.
2. Enter the **rasman type value** *message_type* command at the command line. For example, enter the following command to display all AUDIT messages.

```
device# rasman type value AUDIT
RAS Message        ID             Severity Message
-------------------------------------------------------------------------------------------
-----------------
FCIP-1002          INFO          An IPsec/IKE policy was added
FCIP-1003          INFO          An IPsec/IKE policy was deleted
AUTH-1045          ERROR          Certificate not present in this switch in %s port %d.
AUTH-1046          INFO          %s has been successfully completed.
AUTH-1047          ERROR          %s has failed.
AUTH-3001          INFO          Event: %s, Status: success, Info: %s type has been
changed from [%s] to [%s].
AUTH-3002          INFO          Event: %s, Status: success, Info: %s.
AUTH-3003          INFO          Event: %s, Status: success, Info: %s the PKI objects.
[...]
```

Viewing, clearing, and configuring AUDIT log messages

This section provides information on viewing, clearing, and configuring the AUDIT log messages.

Displaying the AUDIT messages

To display the saved AUDIT messages, perform the following steps.

1. Log in to the switch as admin.
2. Enter the **show logging auditlog** command at the command line.

You can also display messages in reverse order by using the **reverse** option.

```
device# show logging auditlog
[...]
701 AUDIT, 2024/05/04-04:39:40 (GMT), [DCM-1006], INFO, DCMCFG, admin/admin/
134.141.245.254/telnet/cli,, dutA, Event: database commit transaction, Status:
Succeeded, User command: "configure config interface tunnel 1001".

702 AUDIT, 2024/05/04-04:49:35 (GMT), [SEC-3022], INFO, SECURITY, admin/admin/
134.141.245.254/telnet/CLI,, SLX9740-80C, Event: logout, Status: success, Info:
Successful logout by user [admin].

703 AUDIT, 2024/05/04-04:50:32 (GMT), [SEC-3021], INFO, SECURITY, admin/NONE/
134.141.245.254/telnet/CLI,, dutA, Event: login, Status: failed, Info: Failed login
attempt through REMOTE, IP Addr: 134.141.245.254.

704 AUDIT, 2024/05/04-04:51:09 (GMT), [SEC-3020], INFO, SECURITY, admin/admin/
134.141.245.254/telnet/CLI,, SLX9740-80C, Event: login, Status: success, Info:
Successful login attempt via REMOTE, IP Addr: 134.141.245.254.

705 AUDIT, 2024/05/04-05:01:19 (GMT), [SEC-3022], INFO, SECURITY, admin/admin/
134.141.245.254/telnet/CLI,, SLX9740-80C, Event: logout, Status: success, Info:
Successful logout by user [admin].

706 AUDIT, 2024/05/04-16:15:42 (GMT), [SEC-3020], INFO, SECURITY, admin/admin/
134.141.219.41/telnet/CLI,, SLX9740-80C, Event: login, Status: success, Info:
Successful login attempt via REMOTE, IP Addr: 134.141.219.41.

707 AUDIT, 2024/05/04-16:16:41 (GMT), [SEC-3030], INFO, SECURITY, admin/admin/
134.141.245.254/telnet/cli,, SLX9740-80C, Event: secCertUtil, Status: success, Info:
Deleted certificate - https.

708 AUDIT, 2024/05/04-16:16:51 (GMT), [WEBD-3002], INFO, SECURITY, NONE/root/NONE/None/
CLI,, dutA, Event: HTTPS Server, Status: success, Info: HTTPS Server is stopped on all
VRFs due to HTTPS Host certificate removal.

709 AUDIT, 2024/05/04-16:16:51 (GMT), [SEC-3131], INFO, SECURITY, admin/admin/
134.141.219.41/telnet/cli,, dutA, Event: Crypto Ca https, Status: success, Info: Host
certificate and Private key, imported via PKCS#12 bundle are now deleted.

710 AUDIT, 2024/05/04-16:19:00 (GMT), [SEC-3030], INFO, SECURITY, admin/admin/
134.141.219.41/telnet/cli,, SLX9740-80C, Event: secCertUtil, Status: success, Info:
Imported certificate - https.pfx from host 10.20.55.129.

711 AUDIT, 2024/05/04-16:19:00 (GMT), [SEC-3130], INFO, SECURITY, admin/admin/
134.141.219.41/telnet/cli,, dutA, Event: Crypto Ca https, Status: success, Info: Host
certificate and Private key are imported in PKCS#12 file format.

712 AUDIT, 2024/05/04-16:20:39 (GMT), [WEBD-3000], INFO, SECURITY, admin/admin/
134.141.219.41/telnet/cli,, dutA, Event: HTTP(S) Server, Status: success, Info:
HTTP(S) Server instance is started on mgmt-vrf VRF.

713 AUDIT, 2024/05/04-16:20:39 (GMT), [DCM-1006], INFO, DCMCFG, admin/admin/
134.141.219.41/telnet/cli,, dutA, Event: database commit transaction, Status:
Succeeded, User command: "configure config no http server use-vrf mgmt-vrf shutdown".

714 AUDIT, 2024/05/04-16:21:00 (GMT), [WEBD-3000], INFO, SECURITY, admin/admin/
134.141.219.41/telnet/cli,, dutA, Event: HTTP(S) Server, Status: success, Info:
HTTP(S) Server instance is started on default-vrf VRF.

715 AUDIT, 2024/05/04-16:21:00 (GMT), [DCM-1006], INFO, DCMCFG, admin/admin/
134.141.219.41/telnet/cli,, dutA, Event: database commit transaction, Status:
Succeeded, User command: "configure config no http server use-vrf default-vrf
shutdown".
```

```
716 AUDIT, 2024/05/04-16:29:14 (GMT), [TS-1009], INFO, SECURITY, admin/admin/
134.141.219.41/telnet/cli,, dutA, Event: change time: attempt.

717 AUDIT, 2024/05/04-16:29:14 (GMT), [TS-1010], INFO, SECURITY, admin/admin/
134.141.219.41/telnet/cli,, dutA, Event: change time: success, Info:  from 2024-05-04
16:29:14 to 2024-05-15 23:59:59.

718 AUDIT, 2024/05/16-00:00:46 (GMT), [SEC-3136], WARNING,
SECURITY, NONE/NONE/NONE/None/CLI,, dutA, Event: cert expiry , Alert-
level:CRITICAL, Certificate Details=[subject= /C=IN/ST=CHENNAI/L=Madras/O=Extreme/
OU=HCL/CN=10.20.55.129 issuer= /C=IN/ST=CHENNAI/L=Madras/O=Extreme/OU=HCL/CN=Extreme
Root CA/emailAddress=abalan@extreme.com serial=1000] will expire in 3 days.

719 AUDIT, 2024/05/16-00:03:07 (GMT), [TS-1009], INFO, SECURITY, admin/admin/
134.141.219.41/telnet/cli,, dutA, Event: change time: attempt.

720 AUDIT, 2024/05/16-00:03:07 (GMT), [TS-1010], INFO, SECURITY, admin/admin/
134.141.219.41/telnet/cli,, dutA, Event: change time: success, Info:  from 2024-05-16
00:03:07 to 2024-04-15 23:59:59.

721 AUDIT, 2024/04/16-00:00:52 (GMT), [SEC-3136], WARNING,
SECURITY, NONE/NONE/NONE/None/CLI,, dutA, Event: cert expiry , Alert-
level:MINOR, Certificate Details=[subject= /C=IN/ST=CHENNAI/L=Madras/O=Extreme/OU=HCL/
CN=10.20.55.129 issuer= /C=IN/ST=CHENNAI/L=Madras/O=Extreme/OU=HCL/CN=Extreme Root CA/
emailAddress=abalan@extreme.com serial=1000] will expire in 33 days.

722 AUDIT, 2024/04/16-00:06:07 (GMT), [TS-1009], INFO, SECURITY, admin/admin/
134.141.219.41/telnet/cli,, dutA, Event: change time: attempt.

723 AUDIT, 2024/04/16-00:06:07 (GMT), [TS-1010], INFO, SECURITY, admin/admin/
134.141.219.41/telnet/cli,, dutA, Event: change time: success, Info:  from 2024-04-16
00:06:07 to 2024-04-25 23:59:59.

724 AUDIT, 2024/04/26-00:00:53 (GMT), [SEC-3136], WARNING,
SECURITY, NONE/NONE/NONE/None/CLI,, dutA, Event: cert expiry , Alert-
level:MAJOR, Certificate Details=[subject= /C=IN/ST=CHENNAI/L=Madras/O=Extreme/OU=HCL/
CN=10.20.55.129 issuer= /C=IN/ST=CHENNAI/L=Madras/O=Extreme/OU=HCL/CN=Extreme Root CA/
emailAddress=abalan@extreme.com serial=1000] will expire in 23 days.

725 AUDIT, 2024/04/26-00:15:51 (GMT), [SEC-3022], INFO, SECURITY, admin/admin/
134.141.219.41/telnet/CLI,, SLX9740-80C, Event: logout, Status: success, Info:
Successful logout by user [admin].

726 AUDIT, 2024/04/27-00:00:02 (GMT), [SEC-3136], WARNING, SECURITY, NONE/NONE/NONE/
None/CLI,, dutA, Event: cert expiry , Alert-level:INFO, Certificate Details=[subject= /
C=IN/ST=CHENNAI/L=Madras/O=Extreme/OU=HCL/CN=10.20.55.129 issuer= /C=IN/ST=CHENNAI/
L=Madras/O=Extreme/OU=HCL/CN=Extreme Root CA/emailAddress=abalan@extreme.com
serial=1000] will expire in 22 days.

727 AUDIT, 2024/04/27-02:32:59 (GMT), [SEC-3020], INFO, SECURITY, admin/admin/
134.141.245.254/telnet/CLI,, SLX9740-80C, Event: login, Status: success, Info:
Successful login attempt via REMOTE, IP Addr: 134.141.245.254.

728 AUDIT, 2024/04/27-02:48:30 (GMT), [SEC-3022], INFO, SECURITY, admin/admin/
134.141.245.254/telnet/CLI,, SLX9740-80C, Event: logout, Status: success, Info:
Successful logout by user [admin].

729 AUDIT, 2024/04/27-02:48:40 (GMT), [SEC-3020], INFO, SECURITY, admin/admin/
134.141.245.254/telnet/CLI,, SLX9740-80C, Event: login, Status: success, Info:
Successful login attempt via REMOTE, IP Addr: 134.141.245.254.

730 AUDIT, 2024/04/27-03:15:52 (GMT), [SEC-3022], INFO, SECURITY, admin/admin/
134.141.245.254/telnet/CLI,, SLX9740-80C, Event: logout, Status: success, Info:
```

```
Successful logout by user [admin].
[...]
```

Clearing the AUDIT messages

To clear the AUDIT log messages for a particular switch instance, perform the following steps.

1. Log in to the switch as admin.
2. Enter the **clear logging auditlog** command to clear all messages in the switch memory.

Configuring event auditing

The AUDIT log classes SECURITY, CONFIGURATION, and FIRMWARE are enabled by default. You can enable or disable auditing of these classes by using the **logging auditlog class** class command.

To configure and verify the event auditing, perform the following steps.

1. Enter the **configure terminal** command to access the global configuration level of the CLI.
   ```
   device# configure terminal
   Entering configuration mode terminal
   ```
2. Configure the event classes you want to audit. For example, to audit the CONFIGURATON class, enter the following command.

   You can choose one of the following event classes: CONFIGURATION, FIRMWARE, or SECURITY.
   ```
   device(config)# logging auditlog class CONFIGURATION
   ```
3. Enter the **show running-config logging auditlog class** command to verify the configuration.
   ```
   device# show running-config logging auditlog class
   logging auditlog class CONFIGURATION
   ```

Understanding RASLog messages

This section provides information on the RASLog message format.

RASLog messages

The following example shows the format of a RASLog message.

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

The following example shows the sample messages from the log.

```
[...]
2023/04/27-02:48:30, [SEC-3022], 7,, INFO, SLX9740-80C, Event: logout, Status: success,
Info: Successful logout by user [admin].
2023/04/27-02:48:40, [SEC-1206], 8,, INFO, SLX9740-80C, Login information: User [admin
via telnet] Last Successful Login Time : Sat Apr 27 02:32:59 2023.
2023/04/27-02:48:40, [SEC-1203], 9,, INFO, SLX9740-80C, Login information: User [admin]
```

```
Login successful via TELNET/SSH/RSH. IP Addr: 134.141.245.254.
2023/04/27-03:15:52, [SEC-3022], 10,, INFO, SLX9740-80C, Event: logout, Status: success,
Info: Successful logout by user [admin].
[...]
```

The following table describes the fields in the error message.

Table 10: RAS message field description

Variable name	Description
Timestamp	The system time (UTC) when the message was generated on the switch. The RASLog subsystem supports an internationalized time stamp format that is based on the "LOCAL" setting.
Event ID	The Event ID, which is the message module and number. These values uniquely identify each message in SLX-OS and reference the cause and actions recommended in this document. Note that not all message numbers are used; the numeric message sequence can contain gaps.
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 **`firmware download`** operation and increases to a value of as much as 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 message sequence numbering is not split for the system and DCE message logs. The sequence number can be reset to 1 by using the **`clear logging raslog`** command. However, the sequence number is not reset if you clear a particular message type, for example, DCE. The sequence number is persistent across power cycles and switch reboots.
Flags	For most messages, a space character (null value) indicating that the message is neither a DCE or FFDC message. Messages may contain the following values: • DCE: Indicates a message generated by the protocol-based modules. • FFDC: Indicates that additional first failure data capture information has also been generated for this event.
Severity	The severity level of the message, which can be one of the following: • CRITICAL • ERROR • WARNING • INFO
Switch name	The defined switch name or chassis name of the switch. This value is truncated if it exceeds 16 characters.
Event-specific information	A text string explaining the error encountered and providing the parameters supplied by the software at run time.

AUDIT event messages

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

The following example shows the format of the AUDIT event message.

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

The following is a sample AUDIT event message.

```
730 AUDIT, 2024/04/27-03:15:52 (GMT), [SEC-3022], INFO, SECURITY,
admin/admin/134.141.245.254/telnet/CLI,, SLX9740-80C, Event: logout, Status: success,
Info: Successful logout by user [admin].
```

The following table describes the fields in the AUDIT event message.

Table 11: AUDIT message field description

Variable name	Description
Sequence Number	The error message position in the log.
AUDIT	An AUDIT message.
Timestamp	The system time (UTC) when the message was generated on the switch. The RASLog subsystem supports an internationalized time stamp format that is based on the “LOCAL” setting.
Event ID	The Event ID, which is the message module and number. These values uniquely identify each message in the SLX-OS and reference the cause and actions recommended in this document. Note that not all message numbers are used; the numeric message sequence can contain gaps.
Severity	The severity level of the message, which can be one of the following: • CRITICAL • ERROR • WARNING • INFO
Event Class	The event class, which can be one of the following: • DCMCFG • FIRMWARE • SECURITY
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.
Reserved field for future expansion	This field is reserved for future use and contains a space character (null value).

Table 11: AUDIT message field description (continued)

Variable name	Description
Switch name	The defined switch name or chassis name of the switch. This value is truncated if it is over 16 characters.
Event-specific information	A text string explaining the error encountered and providing the parameters supplied by the software at runtime.

Responding to a RASLog message

This section provides procedures on gathering information on RASLog messages.

Looking up a message: This document arranges messages alphabetically by Module ID and then numerically within a given module. To look up a message, copy the module (see Table 9 System module descriptions) and error code and compare them with the Table of Contents or look up 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

Perform the following steps and ask yourself these questions when troubleshooting a system:

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

- Is the switch down?

- How large is the fabric?

- Is the fabric redundant?

• Execute the **`show logging raslog`** command on each switch.

• Execute the **`copy support`** command.

• Document the sequence of events by answering the following questions:

- What happened just before the problem?

- Is the problem repeatable?

- If so, what are the steps to produce the problem?

- What configuration was in place when the problem occurred?

• Was Power-On Self-Test (POST) enabled?

• Are serial port (console) logs available?

• What and when were the last actions or changes made to the system?

Support

SLX-OS creates several files that can help support personnel troubleshoot and diagnose a problem. This section describes those files and how to access and save the information for support personnel.

Panic dump, core dump, and FFDC data files: SLX-OS creates panic dump files, core files, and FFDC data files when problems in the SLX-OS kernel occur. You can view files by using the **`show support`** command. These files can build up in persistent storage and may need to be periodically deleted or downloaded by using the **`copy support`** command.

The software watchdog (SWD) process 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.

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

Enter the **`show support`** command to view these files or the **`copy support ftp`** command to send them to a host workstation using FTP. The panic dump files, core files, and FFDC data files are intended for support personnel use only.

Trace dumps: SLX-OS produces trace dumps when problems are encountered within SLX-OS modules. The SLX-OS trace dump files are intended for support personnel use only. You can use the **`copy support`** command to collect trace dump files to a specified remote location to provide support when requested.

Using the **`copy support`** command: The **`copy support`** command is used to send the output of the RASLog messages, trace files, and output of the **`copy support`** command to an off-switch storage location through FTP. You can upload support save data from the local switch to an external host or save the data on an attached USB device. The **`copy support`** command runs a large number of dump and show commands to provide a global output of the status of the switch. Refer to the *Extreme SLX-OS Command Reference* for more information on the copy support command.

System module descriptions

Table 9 provides a summary of the system modules for which messages are documented in this reference documentation; a module is a subsystem in the SLX-OS. Each module generates a set of numbered messages.

Table 12: System module descriptions

System module	Description
AUTH	AUTH messages indicate problems with the authentication module of the SLX-OS.
BFD	BFD messages indicate whether the BFD session is up or down for the specific neighbors on the interface.
BGP	BGP messages indicate problems with the Border Gateway Protocol (BGP) module of the SLX-OS.
BL	BL messages are a result of faulty hardware, transient out-of-memory conditions, ASIC errors, or inconsistencies in the software state between an interface module and the environment monitor (EM) module.
BLL	Bloom is the name of the ASIC used as the building block for third-generation hardware platforms.
CHS	CHS (CHASSIS) messages report the problems in the management of the interface modules in the different slots of the chassis.
DAD	DAD messages report errors encountered during the DHCP Auto Deployment (DAD) process.
DCM	Distributed Configuration Manager (DCM) messages indicate major switch bootup events, user login or logout, and the configuration operations.
ELD	End Loop Detection (ELD) messages notify a loop in the Layer 2 network and the status of the port on which the loop is detected.
EM	The environmental monitor (EM) manages and monitors the various field-replaceable units (FRUs), including the port cards, blower assemblies, power supplies, and World Wide Name (WWN) cards. EM controls the state of the FRUs during system start-up, hot-plug sequences, and fault recovery. EM provides access to and monitors the sensor and status data from the FRUs and maintains the integrity of the system by using the environmental and power policies. EM reflects system status by way of CLI commands, system light emitting diodes (LEDs), and status and alarm messages. EM also manages some component-related data.
ERCP	ERCP (ERRCAP) messages indicate any problems associated with Double Data Rate (DDR) errors.
FABS	FABS messages indicate problems in the fabric system driver module.
FSS	The fabric state synchronization framework provides facilities by which the active management module can synchronize with the standby management module, enabling the standby management module 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 service. A component is a module in the SLX-OS, implementing a related set of functionality. A service is a collection of components grouped together to achieve a modular software architecture.

Table 12: System module descriptions (continued)

System module	Description
FW	FW messages indicate the warnings when the temperature, voltage, fan speed, and switch status thresholds are exceeded for the switch subsystems.
HASM	HASM is the infrastructure for the High Availability System Management, which has the functionality to maintain the cluster of high-availability switch platforms, deploy and start multiple service instances with active and standby redundancy in a distributed clustering environment, manage the state synchronization and the non-disruptive between active and standby management modules, host the nondisruptive firmware upgrade context, and support the software watchdog and daemon restart.
HIL	HIL messages indicate any issues associated with the Hardware Independent Layer (HIL) for general platform components, such as Environmental Monitoring (EM), fan and power supply unit (PSU) subsystems, and other platform FRUs.
HSL	HSL messages indicate problems with the Hardware Subsystem Layer (HSL) of the SLX-OS.
IGMP	IGMP messages indicate any issue that is associated with the Internet Group Management Protocol (IGMP) snooping feature.
IPAD	IPAD messages are generated by the IP admin demon.
KTRC	KTRC messages indicate any problem that is associated with the RAS-TRACE facility, which provide Extreme Networks internal information to diagnose a failure.
L2AG	L2AG messages indicate problems with the Layer 2 system agent module. L2SS and L2AG, together, control the Layer 2 forwarding engine and are responsible for MAC learning, aging, and forwarding functionalities.
L2SS	L2SS messages indicate problems with the Layer 2 system manager module. L2SS and L2AG, together, control the Layer 2 forwarding engine and are responsible for MAC learning, aging, and forwarding functionalities.
LACP	LACP error messages indicate problems with the Link Aggregation Control Protocol module of the SLX-OS.
LIC	LIC messages indicate problems with the licensing module.
LOG	LOG messages describe events and problems that are associated with the RASLog and AUDIT log facilities.
MCST	MCST messages indicate any problems that are associated with the Layer 2 and Layer 3.
MAPS	The MAPS module identifies and reports anomalies that are associated with the various error counters, thresholds, and resources monitored on the switch.
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.
MSTP	MSTP messages indicate problems with Multiple Spanning Tree Protocol (MSTP) modules of the SLX-OS.
NSM	NSM messages indicate problems with the interface management and VLAN management module of the SLX-OS.

Table 12: System module descriptions (continued)

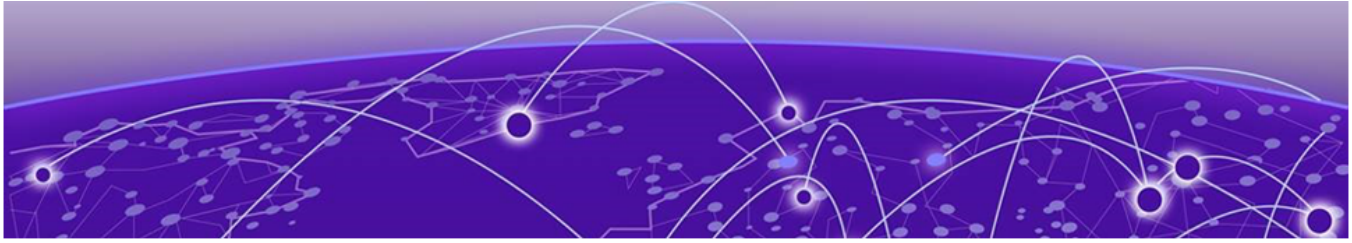
System module	Description
OFMA	The OpenFlow agent module is responsible for mapping the OpenFlow logical view to physical hardware. Any mapping error or unsupported constructs are logged by these messages.
OFMM	OpenFlow manager messages indicate any error in the flow, group, meter mod processing by the OpenFlow subsystem. These include protocol error and VDX pipeline limitations along with the internal error conditions. OpenFlow protocol exchanges and connections are also logged through this module.
ONMD	ONMD messages indicate problems with the Operation, Administration and Maintenance module of the SLX-OS.
OSPF	OSPF messages indicate information or problems with the OSPF module of the SLX-OS.
OSPF6	OSPF6 messages indicate information or problems with the OSPF version 3 module of the SLX-OS.
PCAP	PCAP messages indicate the status or information about the packet capture module.
PDM	Parity data manager (PDM) is a user-space daemon that is responsible for the replication of persistent configuration files from the primary partition to the secondary partition and from the active management module to the standby management module.
PHP	PHP messages indicate any important information that is associated with the discovery and creation, deletion, and updating of the port profiles.
PIM	PIM messages indicate problems with the Protocol-Independent Multicast (PIM) module.
PLAT	PLAT messages indicate hardware problems.
PORT	PORT 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.
QOSD	QOSD messages indicate problems with the Quality of Service (QoS) module.
RAS	RAS messages notify when first failure data capture (FFDC) events are logged to the FFDC log and size or roll-over warnings.
RPS	Route Processor Source (RPS) messages contain message route map information, such as route map status and the message source address, message group address, and route processor address.
RTM	Route Manager (RTM) messages indicate status or errors while updating or maintaining the route and next-hop database.
SCN	The internal State Change Notification (SCN) daemon is used for state change notifications from the kernel to the daemons within SLX-OS.
SEC	SEC messages indicate security errors, warnings, or information during security-related data management or fabric merge operations. Administrators must watch for these messages to distinguish between internal switch and fabric operation errors and external attack.

Table 12: System module descriptions (continued)

System module	Description
SFLO	sFlow is a standards-based sampling technology embedded within switches and routers, which is used to monitor high-speed network traffic. sFlow uses two types of sampling: • Statistical packet-based sampling of switched or routed packet flows. • Time-based sampling of interface counters. SFLO messages indicate errors or information related to the sFlow daemon.
SLCD	SLCD messages provide wear-level statistics of the western digital (WD) SiliconDrive 2 compact flash.
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. Extreme Networks switches support four management entities that can be configured to receive these traps or informs. SNMP messages indicate problems in the SNMP operations.
SRM	System Resource Monitor daemon monitors memory and CPU usage of all processes. The SRM message is generated when the available low memory is below 100 MB.
SS	SS messages indicate problems during the execution of the **`copy support`** command.
SSMD	SSMD messages indicate problems with the System Services Module (SSM) of the SLX-OS.
SULB	The software upgrade library provides the **`firmware download`** command capability, which enables firmware upgrades and nondisruptive code load to the switches. SULB messages may be displayed if there are any problems during the firmware download procedure.
SWCH	SWCH messages are generated by the switch driver module that manages a Fibre Channel switch instance.
TNLD	TNLD messages indicate status or problems with the Data Center Ethernet (DCE) tunnel manager of the SLX-OS.
TOAM	TRILL OAM (TOAM) messages indicate problems with the **`l2traceroute`** family of commands that help in the troubleshooting of cluster data paths.
TRCE	TRCE messages describe events and problems that are associated with the tracedump facility.
TS	Time Service (TS) provides switch time synchronization by synchronizing all clocks in the network. The TS messages indicate information or errors during the switch time synchronization.
UCST	UCST is a part of the fabric shortest path first (FSPF) protocol that manages the unicast routing table.
UDLD	UDLD messages indicate problems with the UniDirectional Link Detection (UDLD) module of the SLX-OS.
UPTH	UPATH is a part of the FSPF protocol that uses the SPF algorithm to dynamically compute a unicast tree.

Table 12: System module descriptions (continued)

System module	Description
VC	VC messages indicate any important information related to the CLI and its plug-ins.
VRRP	VRRP messages indicate information or problems with the VRRP module of the SLX-OS.
WEBD	WEBD messages Indicate problems with the Web Tools module.
WLV	Wolverine (WLV) ASIC is a component that connects the front-end port. WLV messages indicate failures in the front-end port.



SLX-OS Modules

ARP Messages on page 70
AUTH Messages on page 71
BFD Messages on page 85
BGP Messages on page 87
BL Messages on page 94
BLL Messages on page 110
CHS Messages on page 111
DAD Messages on page 112
DCM Messages on page 121
DOT1 Messages on page 140
ELD Messages on page 144
EM Messages on page 147
ERCP Messages on page 163
FABS Messages on page 163
FSS Messages on page 168
FW Messages on page 172
HASM Messages on page 199
HIL Messages on page 208
HSL Messages on page 218
IGMP Messages on page 226
IPAD Messages on page 227
IPHL Messages on page 229
KTRC Messages on page 231
L2AG Messages on page 233
L2SS Messages on page 236
LACP Messages on page 243
LIC Messages on page 245
LOG Messages on page 246
MAPS Messages on page 250
MCST Messages on page 259
MM Messages on page 265
MPTH Messages on page 265
MSTP Messages on page 266
NSM Messages on page 269

OFMA Messages on page 300
OFD Messages on page 300
ONMD Messages on page 302
OSPF Messages on page 304
OSPF6 Messages on page 306
PCAP Messages on page 306
PDM Messages on page 307
PHP Messages on page 312
PIM Messages on page 313
PLAT Messages on page 313
PORT Messages on page 317
QOSD Messages on page 320
RADV Messages on page 324
RAS Messages on page 328
RPS Messages on page 334
RTM Messages on page 335
SCN Messages on page 338
SEC Messages on page 339
SFLO Messages on page 376
SLCD Messages on page 382
SNMP Messages on page 385
SRM Messages on page 386
SS Messages on page 388
SSMD Messages on page 393
SULB Messages on page 401
SWCH Messages on page 409
TNDL Messages on page 412
TOAM Messages on page 415
TRCE Messages on page 416
TS Messages on page 419
UCST Messages on page 421
UDLD Messages on page 422
UPTH Messages on page 424
VRRP Messages on page 424
WEBD Messages on page 437

ARP Messages

ARP-1042

Message: `[ IPv6 | IPv4 ] Hosts have reached the high threshold limit of <high-threshold-value>.`

Message Type: INFO

Severity: INFO

Probable Cause: The number of IPv6/IPv4 hosts in the host table has reached the user configured high threshold limit.

Recommended Action: Reduce the number of hosts stored in the table.

ARP-1043

Message: `[ IPV6 | IPv4 ] Hosts have dropped below the low threshold limit of <low-threshold-value >.`

Message Type: INFO

Severity: INFO

Probable Cause: The number of IPv6/IPv4 hosts in the host table has dropped below the user configured low threshold limit.

Recommended Action: No action is required.

AUTH Messages

AUTH-1001

Message: `<Operation type> has been successfully completed.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that the secret database has been updated using the **`fcsp auth-secret`** or **`no fcsp auth-secret`** command. The values for Operation type can be "set" or "remove".

Recommended Action: No action is required.

AUTH-1002

Message:`<Operation type> has failed.`

Message Type: LOG

Severity: ERROR

Probable Cause: Indicates that the specified action to update the secret database using the **`fcsp auth-secret`** or **`no fcsp auth-secret`** command has failed. The values for Operation type can be "set" or "remove".

Recommended Action: Execute the **fcsp auth-secret** or **no fcsp auth-secret** command again. Execute the **copy support** command and contact your switch service provider.

AUTH-1003

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

Message Type: LOG

Severity:INFO

Probable Cause: Indicates that an authentication configuration parameter was set to a specified value. The data type can be either authentication type, DH group type, or policy type.

Recommended Action: No action is required.

AUTH-1004

Message: `Failed to set <data type> type to <setting value>.`

Message Type: LOG

Severity: ERROR

Probable Cause: Indicates that the **fcsp auth** command has failed to set the authentication configuration value. The data type can be either authentication type, DH group type, hash type, or policy type.

Recommended Action: Execute the **fcsp auth** command. Execute the **copy support** command and contact your switch service provider.

AUTH-1006

Message: `Failed to open authentication configuration file.`

Message Type: LOG

Severity:WARNING

Probable Cause: Indicates an internal problem with the security policy.

Recommended Action: Reinitialize authentication using the **shutdown** and **no shutdown** commands or the **chassis disable** and **chassis enable** commands. If the message persists, execute the **copy support** command and contact your switch service provider.

AUTH-1007

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

Message Type: LOG

Severity:ERROR

Probable Cause: Indicates that the proposed authentication protocol types are not supported by the local port.

Recommended Action: Execute the **`fcsp auth`** command to make sure the local switch supports the following protocols: Fibre Channel Authentication Protocol (FCAP) or Diffie-Hellman Challenge Handshake Authentication Protocol (DH-CHAP).

AUTH-1010

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

Message Type: LOG

Severity:ERROR

Probable Cause: Indicates an internal problem with the security policy.

Recommended Action: Reload or power cycle the switch. If the message persists, execute the **`copy support`** 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

Severity:WARNING

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

Recommended Action: Make sure the entity at the other end of the link supports authentication.

AUTH-1013

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

Message Type: LOG

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 **shutdown** and **no shutdown** commands or the **chassis disable** and **chassis enable** commands.

If the message persists, execute the **copy support** command and contact your switch service provider.

AUTH-1014

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

Message Type:LOG | FFDC

Severity:ERROR

Probable Cause: Indicates an internal problem with the security policy.

Recommended Action: Reinitialize authentication using the **shutdown** and **no shutdown** commands or the **chassis disable** and **chassis enable** commands. If the message persists, execute the **copy support** 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

Severity: ERROR

Probable Cause: Indicates an internal problem with the security policy.

Recommended Action: Reinitialize authentication using the **shutdown** and **no shutdown** commands or the **chassis disable** and **chassis enable** commands. If the message persists, execute the **copy support** command and contact your switch service provider.

AUTH-1018

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

Message Type: LOG

Severity:ERROR

Probable Cause: Indicates an internal problem with the security policy.

Recommended Action: Reinitialize authentication using the **shutdown** and **no shutdown** commands or the **chassis disable** and **chassis enable** commands. If the message persists, execute the **copy support** command and contact your switch service provider.

AUTH-1020

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

Message Type: LOG

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 **shutdown** and **no shutdown** commands or the **chassis disable** and **chassis enable** commands. If the message persists, execute the **copy support** command and contact your switch service provider.

AUTH-1022

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

Message Type: LOG

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 **shutdown** and **no shutdown** commands or the **chassis disable** and **chassis enable** commands. If the message persists, execute the **copy support** command and contact your switch service provider.

AUTH-1025

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

Message Type: LOG

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 **shutdown** and **no shutdown** commands or the **chassis disable** and **chassis enable** commands. If the message persists, execute the **copy support** command and contact your switch service provider.

AUTH-1026

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

Message Type: LOG

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. The authentication may fail.

Recommended Action: Reinitialize authentication using the **shutdown** and **no shutdown** commands or the **chassis disable** and **chassis enable** commands. If the message persists, execute the **copy support** 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

Severity:ERROR

Probable Cause: Indicates that the authentication process failed to select an authentication value (for example, DH group, hash value, or protocol type) from a receiving payload during the specified authentication phase. This error occurred because 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 **fcsp auth** command. Reinitialize authentication using the **shutdown** and **no shutdown** commands or the **chassis disable** and **chassis enable** commands. If the message persists, execute the **copy support** command and contact your switch service provider.

AUTH-1028

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

Message Type: LOG

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 a 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 **shutdown** and **no shutdown** commands or the **chassis disable** and **chassis enable** commands. If the message persists, execute the **copy support** 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

Severity:ERROR

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

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

Recommended Action: Reinitialize authentication using the **shutdown** and **no shutdown** commands or the **chassis disable** and **chassis enable** commands.

If the message persists, execute the **copy support** command and contact your switch service provider.

AUTH-1030

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

Message Type: LOG

Severity:ERROR

Probable Cause: Indicates that the receiving payload does not have a valid message code during the specified authentication phase. Usually this problem is transient. The authentication may fail.

Recommended Action: Reinitialize authentication using the **shutdown** and **no shutdown** commands or the **chassis disable** and **chassis enable** commands.

If the message persists, execute the **copy support** command and contact your switch service provider.

AUTH-1031

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

Message Type: LOG

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 **`fcsp auth-secret`** command.

Reinitialize authentication using the **`shutdown`** and **`no shutdown`** commands or the **`chassis disable`** and **`chassis enable`** commands.

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

Severity:ERROR

Probable Cause: Indicates that the authentication process failed to generate specific data (for example, 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 **`shutdown`** and **`no shutdown`** commands or the **`chassis disable`** and **`chassis enable`** commands.

If the message persists, execute the **`copy support`** command and contact your switch service provider.

AUTH-1033

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

Message Type: LOG

Severity: ERROR

Probable Cause: Indicates that an entity, which was not configured in the switch connection control (SCC) policy tried to connect to the port.

Recommended Action: Add the entity World Wide Name (WWN) to the SCC policy using the **`secpolicy defined-policy`** command, then reinitialize authentication using the **`shutdown`** and **`no shutdown`** commands or the **`chassis disable`** and **`chassis enable`** commands.

AUTH-1034

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

Message Type: LOG

Severity:ERROR

Probable Cause: Indicates that the entity name in the payload is not in the correct format.

Recommended Action: Reinitialize authentication using the **`shutdown`** and **`no shutdown`** commands or the **`chassis disable`** and **`chassis enable`** commands.

If the message persists, execute the **`copy support`** 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

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 **`shutdown`** and **`no shutdown`** commands or the **`chassis disable`** and **`chassis disable`** commands.

If the message persists, execute the **`copy support`** command and contact your switch service provider.

AUTH-1036

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

Message Type: LOG

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 **`shutdown`** and **`no shutdown`** commands or the **`chassis disable`** and **`chassis disable`** commands.

If the message persists, execute the **copy support** 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

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. 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.

Reinitialize authentication using the **shutdown** and **no shutdown** commands or the **chassis disable** and **chassis disable** commands.

If the message persists, execute the **copy support** command and contact your switch service provider.

AUTH-1039

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

Message Type: LOG

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 **fcsp auth** command, and then enable the port using the **no shutdown** command.

AUTH-1040

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

Message Type: LOG

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 **fcsp auth** command, and then enable the port on neighboring switch using the **no shutdown** 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

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 **show fcsp auth-secret dh-chap** command and reinitialize authentication using the **shutdown** and **no shutdown** commands or the **chassis disable** and **chassis disable** commands.

If the message persists, execute the **copy support** 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

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 **show fcsp auth-secret dh-chap** command and reinitialize authentication using the **shutdown** and **no shutdown** commands or the **chassis disable** and **chassis disable** commands.

If the message persists, execute the **copy support** command and contact your switch service provider.

AUTH-1044

Message: `Authentication <Reason for disabling the port>. Disabling the port <port number>.`

Message Type: LOG | FFDC

Severity:ERROR

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

Recommended Action: Check the SFP and the cable. Then try to enable the port using the **no shutdown** command.

AUTH-3001

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

Message Type: AUDIT

Class:SECURITY

Severity:INFO

Probable Cause: Indicates that a authentication configuration parameter was set to a specified value. The data type can be either authentication type, DH group type, hash type, or policy type.

Recommended Action: No action is required.

AUTH-3002

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

Message Type: AUDIT

Class:SECURITY

Severity:INFO

Probable Cause: Indicates that the secret database has been updated using the **fcsp auth-secret** command.

Recommended Action: No action is required.

AUTH-3004

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

Message Type: AUDIT

Class:SECURITY

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 **fcsp auth** command, and then enable the port using **no shutdown** 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

Class:SECURITY

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 **fcsp auth** command, and then enable the port on the neighboring switch using **no shutdown** 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 DH-CHAP shared secrets.`

Message Type: AUDIT

Class:SECURITY

Severity:INFO

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. 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 **show fcsp auth-secret dh-chap** command and reinitialize authentication using the **shutdown** and **no shutdown** commands or the **chassis disable** and **chassis enable** commands.

If the message persists, execute the **copy support** command and contact your switch service provider.

AUTH-3007

Message: `Event: <Event Name>, Status: failed, Info: Port <port number> disabled, because an authentication-reject was received with code '<Reason String>' and Explanation '<Explanation String>'.`

Message Type: AUDIT

Class:SECURITY

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 **show fcsp auth-secret dh-chap** and reinitialize authentication using the **shutdown** and **no shutdown** commands or the **chassis disable** and **chassis enable** commands.

If the message persists, execute the **copy support** 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

Class:SECURITY

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 **`show fcsp auth-secret dh-chap`** and reinitialize authentication using the **`shutdown`** and **`no shutdown`** commands or the **`chassis disable`** and **`chassis enable`** commands.

If the message persists, execute the **`copy support`** command and contact your switch service provider.

BFD Messages

BFD-1001

Message: `BFD Session UP for neighbor <NeighborIp> on interface <InterfaceName>.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that the Bidirectional Forwarding Detection (BFD) session for the specified neighbor is now up.

Recommended Action: No action is required.

BFD-1002

Message: `BFD Session DOWN for neighbor <NeighborIp> on interface <InterfaceName> reason <DownReason>.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that the Bidirectional Forwarding Detection (BFD) session for the specified neighbor is now down.

Recommended Action: No action is required.

BFD-1005

Message: `BFD session has reached user configured high threshold limit.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that the number of BFD sessions has exceeded the user configured high threshold level.

Recommended Action: Reduce the number of active BFD sessions.

BFD-1006

Message: `BFD session has dropped below user user configured low threshold limit.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that the number of active BFD sessions has dropped below the user configured low threshold level.

Recommended Action: No action is required.

BFD-1007

Message: `IPv4 BFD session has reached user configured high threshold limit.`

Message Type: LOG

Severity: INFO

Probable Cause: On SLX 9740 and Extreme 8820, indicates that the number of active IPv4 BFD sessions has crossed the user configured high threshold level. Not available on other devices.

Recommended Action: Reduce the number of active IPv4 BFD sessions.

BFD-1008

Message: `IPv4 BFD session has dropped below user user configured low threshold limit.`

Message Type: LOG

Severity: INFO

Probable Cause: On SLX 9740 and Extreme 8820, indicates that the number of active IPv4 BFD sessions has dropped below the user configured low threshold level. Not available on other devices.

Recommended Action: No action is required.

BFD-1009

Message: `IPv6 BFD session has reached user configured high threshold limit.`

Message Type: LOG

Severity: INFO

Probable Cause: On SLX 9740 and Extreme 8820, indicates that the number of active IPv6 BFD sessions has crossed the user configured high threshold level. Not available on other devices.

Recommended Action: Reduce the number of active IPv6 BFD sessions.

BFD-1010

Message: `IPv6 BFD session has dropped below user user configured low threshold limit.`

Message Type: LOG

Severity: INFO

Probable Cause: On SLX 9740 and Extreme 8820, indicates that the number of active IPv6 BFD sessions has dropped below the user configured low threshold level. Not available on other devices.

Recommended Action: No action is required.

BGP Messages

BGP-1001

Message: `<INFO %s>.`

Message Type: LOG

Severity: ERROR

Probable Cause: Indicates a configuration error.

Recommended Action: Make sure to input or pass the right parameter through the CLI or other daemon.

BGP-1002

Message: `<INFO %s %s %s>.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates a Border Gateway Protocol (BGP) interface state change or external link-state database (LSDB) overflow notification.

Recommended Action: No action is required.

BGP-1003

Message: `<ERROR packet error, %s %s>.`

Message Type: LOG

Severity: ERROR

Probable Cause: Indicates that the length, format, or content of the received packet is incorrect.

Recommended Action: Check the configuration at the local or remote node.

BGP-1004

Message: `<INFO BGP: Neighbor %s on VRF %s DOWN (%s)>.`

Message Type: LOG

Severity: WARNING

Probable Cause: Indicates a Border Gateway Protocol (BGP) interface state change or external link-state database (LSDB) overflow warning.

Recommended Action: No action is required.

BGP-1005

Message: `<INFO BGP: Neighbor %s on VRF %s UP (ESTABLISHED)>.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates a Border Gateway Protocol (BGP) Peer Session state UP.

Recommended Action: No action is required.

BGP-1006

Message: `<INFO BGP: Neighbor %s on VRF %s DOWN (%s:%s)>.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates a Border Gateway Protocol (BGP) Peer Session state DOWN.

Recommended Action: No action is required.

BGP-1007

Message: `<CRITICAL BGP Process Restarted Cold>.`

Message Type: LOG

Severity: CRITICAL

Probable Cause: Indicates a Border Gateway Protocol (BGP). Process restarted Cold.

Recommended Action: No action is required.

BGP-1009

Message: `<CRITICAL %s: Memory reached %s>. Review BGP Route scale supported on this platform.`

Message Type: LOG

Severity: WARNING

Probable Cause: Indicates the current memory usage.

Recommended Action: No action is required.

BGP-1011

Message: `< Warning : (%s)BGP EVPN route dampened due to frequent moves >.`

Message Type: LOG

Severity: WARNING

Probable Cause: Indicates routes dampened due to frequent moves.

Recommended Action: No action is required.

BGP-1012

Message: `<BGP : No. of prefix received from BGP peer %s: exceeded %s limit %u>.`

Message Type: LOG

Severity: WARNING

Probable Cause: Indicates no. of prefixes received from a peer have reached max/warning limit.

Recommended Action: No action is required.

BGP-1013

Message: `<WARNING : The stanza %d in the Flowspec route-map %s can not be advertised by BGP, as the NLRI length needed by match criteria is greater than seq_num>.`

Message Type: LOG

Severity: WARNING

Probable Cause: Indicates flowspec route-map can't be advertised by BGP.

Recommended Action: No action is required.

BGP-1014

Message: `<WARNING : The stanza %d in route-map %s is going to be active local %s route as the current active stanza %d with same match and set contentseq_num>.`

Message Type: LOG

Severity: WARNING

Probable Cause:flowspec rule gets generated from dup rmap stanza when the original stanza is modified.

Recommended Action: No action is required.

BGP-1018

Message: `<WARNING : The stanza %d in route-map %s can not form a local %s route as it has same match and set content as current active stanza %d>.`

Message Type: LOG

Severity: WARNING

Probable Cause:flowspec rule is not generated from duplicate rmap stanza.

Recommended Action: No action is required.

BGP-1019

Message: `<WARNING: Not all the prefixes from the in-bound prefix list %s can be sent to %s in ORF message, as there are many prefixes >.`

Message Type: LOG

Severity: WARNING

Probable Cause:BGP ORF Prefix list send limit reached.

Recommended Action: No action is required.

BGP-1020

Message: `<WARNING TCP flags match sub-component is more than a byte in the %s Flowspec rules %s%s%s, so the rule is not listed>.`

Message Type: LOG

Severity: WARNING

Probable Cause:TCP flags match sub-component is more than a byte in the Flowspec rule.

Recommended Action: No action is required.

BGP-1021

Message: `<WARNING: MAC address mismatch for Virtual IP/IPV6 address %s Local MAC: [%s} Recv MAC: [%s] for Interface %s>.`

Message Type: LOG

Severity: WARNING

Probable Cause: Mac-address mismatch.

Recommended Action: No action is required.

BGP-1022

Message: `<WARNING:IP configured is not SAG for IP/IPV6 address %s for Interface: %s>.`

Message Type: LOG

Severity: WARNING

Probable Cause:IP configured is not SAG.

Recommended Action: No action is required.

BGP-1023

Message: `<WARNING: Mismatch for virtual IPV6 address %s Recv MAC: [%s] for Revc tag: [%d]>.`

Message Type: LOG

Severity: WARNING

Probable Cause: Mismatch for virtual IPV6.

Recommended Action: No action is required.

BGP-1024

Message: `<WARNING BGP: afi-%d safi-%d No. of add-path NLRIs for prefix %s/%d received from Peer %s: exceeded maximum limit %d. NLRI 0x%x dropped>.`

Message Type: LOG

Severity: WARNING

Probable Cause:NLRI dropped.

Recommended Action: No action is required.

BGP-1025

Message: `<WARNING BGP: No. of prefix received from BGP peer %s : exceeded Maximum prefix limit. Peer is shutdown>.`

Message Type: LOG

Severity: WARNING

Probable Cause: Peer is shutdown

Recommended Action: No action is required.

BGP-1026

Message: `<INFO BGP : RPKI session for TCP Server: %s on Port : %s is %s. >.`

Message Type: LOG

Severity: WARNING

Probable Cause:RPKI session for TCP Server.

Recommended Action: No action is required.

BGP-1027

Message: `<INFO BGP : RPKI session for SSH Server: %s on Port : %d is %s.>.`

Message Type: LOG

Severity: WARNING

Probable Cause:RPKI session for SSH Server.

Recommended Action: No action is required.

BGP-1028

Message: `<INFO BGP:Neighbor %s on VRF %s enters into Dampened state>.`

Message Type: LOG

Severity: WARNING

Probable Cause:VRF %s enters into Dampened state

Recommended Action: No action is required.

BGP-1029

Message: `<INFO BGP : Neighbor %s on VRF %s Moves out from Dampened state>.`

Message Type: LOG

Severity: WARNING

Probable Cause:VRF %s Moves out from Dampened state.

Recommended Action: No action is required.

BGP-1031

Message: `INFO BGP: Advertise AC-influenced-DF-election capability is enabled on ethernet-segment %ethenet-segment-identifier%`

Message Type: INFO

Severity: INFO

Probable Cause: AF-influenced-DF-election is enabled on a specific ES.

Recommended Action: No action is required.

BGP-1032

Message: `INFO BGP: Advertise AC-influenced-DF-election capability is disabled on ethernet-segment %ethenet-segment-identifier%`

Message Type: INFO

Severity: INFO

Probable Cause: AF-influenced-DF-election is disabled on a specific ES.

Recommended Action: No action is required.

BGP-1033

Message: `INFO BGP: ES route sent with AC-influenced-DF-election for ethernet-segment %ethenet-segment-identifier%`

Message Type: INFO

Severity: INFO

Probable Cause: ES route is sent with the AF-influenced-DF-election attribute for the specified ES.

Recommended Action: No action is required.

BGP-1034

Message: `INFO BGP: DF election is trigged for ethernet-segment %ethenet-segment-identifier%.`

Message Type: INFO

Severity: INFO

Probable Cause: DF election is triggered due to configuration changes for the specified ES.

Recommended Action: No action is required.

BL Messages

BL-1000

Message: `Initializing ports...`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that the switch has started initializing the ports.

Recommended Action: No action is required.

BL-1001

Message:`Port initialization completed.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that the switch has completed initializing the ports.

Recommended Action: No action is required.

BL-1002

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

Message Type: FFDC | LOG

Severity: CRITICAL

Probable Cause: Indicates that the interface module initiation failed because one or more of the internal ports were not online. The interface module is faulted.

Recommended Action: No action is required.

Make sure that the interface module is seated correctly. If the interface module is seated correctly, reload or power cycle the interface module using the **`power-off`** and **`power-on`** commands.

Execute the **`diag systemverification`** command to verify that the interface module does not have hardware problems.

Execute the **`diag post`** command to make sure that Power-On Self-Test (POST) is enabled.

Additional interface module 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 interface module.

BL-1003

Message: `Faulty interface module in <slot string>.`

Message Type: FFDC | LOG

Severity: CRITICAL

Probable Cause: Indicates a faulty interface module in the specified slot chassis.

Recommended Action: Make sure that the interface module is seated correctly. If the interface module is seated correctly, reload or power cycle the interface module using the **power-off** and **power-on** commands.

Execute the **diag systemverification** command to verify that the interface module does not have hardware problems.

Execute the **diag post** command to make sure that Power-On Self-Test (POST) is enabled.

If the message persists, replace the interface module.

BL-1004

Message: `Suppressing interface module fault in <slot string>.`

Message Type: FFDC | LOG

Severity: CRITICAL

Probable Cause: Indicates that the specified interface module experienced a failure but was not faulted due to a user setting.

Recommended Action: Reload or power cycle the interface module using the **power-off** and **power-on** commands.

Execute the **diag systemverification** command to verify that the interface module does not have hardware problems.

Execute the **diag post** command to make sure that Power-On Self-Test (POST) is enabled.

If the message persists, replace the interface module.

BL-1006

Message: `Interface module <slot string number> NOT faulted. Peer interface module <slot string number> experienced abrupt failure.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that the errors (mostly synchronization errors) on this interface module are harmless. Probably, the standby management module connected to the active management module has experienced transitory problems

Recommended Action: Execute the **show ha** command to verify that the standby management module is healthy. If the problem persists, remove and reinstall the faulty interface module.

If the standby management module was removed or faulted by user intervention, no action is required.

BL-1007

Message: `interface module #<interface module number>: state is inconsistent with EM. bl_cflags 0x<interface module control flags>, slot_on <slot_on flag>, slot_off <slot_off flag>, faulty <faulty flag>, status <interface module status>.`

Message Type: LOG

Severity: WARNING

Probable Cause: Indicates that a occurred while an interface module was initializing on the previously active management module.

Recommended Action: No action is required. The interface module is re-initialized. Because re-initializing an interface module is a disruptive operation and can stop I/O traffic, you must stop and restart the traffic during this process.

BL-1008

Message: slot string control-plane failure. Expected value: 0x<value 1>, Actual: 0x<value 2>.

Message Type: FFDC | LOG

Severity: CRITICAL

Probable Cause: Indicates that the interface module has experienced a hardware failure or was removed without following the recommended removal procedure.

Recommended Action: Make sure that the interface module is seated correctly. If the interface module is seated correctly, reload or power cycle the interface module using the **`power-off`** and **`power-on`** commands.

Execute the **`diag systemverification`** command to verify that the interface module does not have hardware problems.

Execute the **`diag post`** command to make sure that Power-On Self-Test (POST) is enabled.

If the message persists, replace the interface module.

BL-1009

Message: `Interface module in <slot number> timed out initializing the chips.`

Message Type: FFDC | LOG

Severity: CRITICAL

Probable Cause: Indicates that the interface module has failed to initialize the application-specific integrated circuit (ASIC) chips.

Recommended Action: Make sure that the interface module is seated correctly. If the interface module is seated correctly, reload or power cycle the interface module using the **power-off** and **power-on** commands.

Execute the **diag systemverification** command to verify that the interface module does not have hardware problems.

Execute the **diag post** command to make sure that Power-On Self-Test (POST) is enabled.

If the message persists, replace the interface module

BL-1010

Message: `Interface module in <slot string> is inconsistent with the hardware settings.`

Message Type: LOG

Severity: WARNING

Probable Cause: Indicates that a occurred while some hardware changes (such as changing the domain ID) were being made on the previously active management module

Recommended Action: No action is required. This interface module has been re-initialized. Because re-initializing an interface module is a disruptive operation and can stop I/O traffic, you must stop and restart the traffic during this process.

BL-1011

Message: `Busy with emb-port int for chip <chip number> in minis <mini-switch number> on interface module <slot number>, chip int is disabled. Interrupt status=0x<interrupt status>.`

Message Type: FFDC | LOG

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 management module 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.

Execute the **diag systemverification** command to verify that the interface module or switch does not have hardware problems.

Execute the **diag post** command to make sure that Power-On Self-Test (POST) is enabled.

For a modular switch, execute the **power-off** and **power-on** commands to power cycle the interface module.

For a compact switch, reload or power cycle the switch.

If the message persists, replace the interface module or the switch.

BL-1012

Message: `bport <interface module port number> port int is disabled. Status=0x<interrupt status>; Port <port number> will be re-enabled in a minute.`

Message Type: LOG

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 management module from becoming too busy. The interface module port number displayed in the message 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.

For a modular switch, execute the **power-off** and **power-on** commands to power cycle the interface module.

For a compact switch, reload or power cycle the switch.

If the message persists, replace the interface module or the switch.

BL-1013

Message: `bport <interface module port number> port is faulted. Status=0x<interrupt status>; Port <port number> will be re-enabled in a minute.`

Message Type: LOG

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 management module from becoming too busy. The interface module port number displayed in the message may not correspond to the 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.

For a modular switch, execute the **power-off** and **power-on** commands to power cycle the interface module.

For a compact switch, reload or power cycle the switch.

If the message persists, replace the interface module or the switch.

BL-1014

Message: `bport <interface module port number> port int is disabled. Status=0x<interrupt status>.`

Message Type: LOG

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 management module from becoming too busy. The interface module port number displayed in the message may not correspond to the user port number.

Recommended Action: Make sure to capture the console output during this process.

For a modular switch, execute the **power-off** and **power-on** commands to power cycle the interface module.

For a compact switch, execute the reload command to reload the switch.

Execute the **diag systemverification** command to determine if there is a hardware error.

Execute the **diag post** command to make sure that Power-On Self-Test (POST) is enabled.

If there is a hardware error, the **power-off** or **power-on** command fails on the modular switch, or the errors are encountered again, replace the interface module or the switch.

BL-1015

Message: `bport <interface module port number> port is faulted. status=0x<interrupt status>.`

Message Type: LOG

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 management module from becoming too busy. The interface module port number displayed in the message may not correspond to the user port number.

Recommended Action: Make sure to capture the console output during this process.

For a modular switch, execute the power-off and power-on commands to power cycle the interface module.

For a compact switch, execute the **reload** command to reload the switch.

Execute the **diag systemverification** command to determine if there is a hardware error.

Execute the **diag post** command to ensure that Power-On Self-Test (POST) is enabled.

If there is a hardware error, the **power-off** or **power-on** command fails on the modular switch, or the errors are encountered again, replace the interface module or the switch.

BL-1016

Message: `Interface module port <port number> in <slot string> failed to enable.`

Message Type: FFDC | LOG

Severity: CRITICAL

Probable Cause: Indicates that the specified interface module port could not be enabled.

Recommended Action: Make sure that the interface module is seated correctly. If the interface module is seated correctly, reload or power cycle the interface module using the power-off and power-on commands.

Execute the **diag systemverification** command to verify that the interface module does not have hardware problems.

Execute the **diag post** command to make sure that Power-On Self-Test (POST) is enabled.

If the message persists, replace the interface module.

BL-1017

Message: `<slot string> Initializing.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that the specified slot chassis has started initializing the ports.

Recommended Action: No action is required.

BL-1018

Message: `<slot string> Initialization completed.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that the specified slot chassis has completed initializing the ports.

Recommended Action: No action is required.

BL-1019

Message: `<slot string>, retry <Retry Number>, internal port retry initialization, <List of internal ports retrying initialization>.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that the specified slot chassis had internal ports that are not online. Initiated a retry on ports that failed to go online.

Recommended Action: No action is required.

BL-1020

Message: `Switch timed out initializing the chips.`

Message Type: LOG | FFDC

Severity: CRITICAL

Probable Cause: Indicates that the switch has failed to initialize the application-specific integrated circuit (ASIC) chips.

Recommended Action: Reload power cycle the switch.

Execute the **`diag systemverification`** command to verify that the switch does not have hardware problems.

Execute the **`diag post`** command to make sure that Power-On Self-Test (POST) is enabled.

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

Severity: INFO

Probable Cause: Indicates that the switch had internal ports that are not online. Initiated a retry on ports that failed to go online.

Recommended Action: No action is required.

BL-1022

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

Message Type: LOG

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: Reload or power cycle the switch.

Execute the **`diag systemverification`** command to verify that the switch does not have hardware problems.

Execute the **`diag post`** command to make sure that Power-On Self-Test (POST) is enabled.

Additional fault messages precede and follow this error providing more information. Refer to other error messages for recommended action.

If the message persists, replace the switch.

BL-1023

Message: `Interface module in <slot string> was reset before initialization completed. As a result the interface module is faulted.`

Message Type: LOG

Severity: CRITICAL

Probable Cause: Indicates that the interface module was reset before the initialization completed.

Recommended Action: Reload or power cycle the interface module using the **`power-off`** and **`power-on`** commands. If the message persists, replace the interface module

Execute the **`diag systemverification`** command to verify that the switch does not have hardware problems.

BL-1024

Message: `All ports on the interface module in <slot string> will be reset as part of the firmware upgrade.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that a recent firmware upgrade caused the interface module firmware to be upgraded and resulted in a cold upgrade. As part of the upgrade, all data path elements were reset.

Recommended Action: No action is required.

BL-1026

Message: `Internal port offline during warm recovery, state <port state> (0x<port ID>).`

Message Type: LOG

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 **`copy support`** command and reload the switch.

Execute the **`diag post`** command to make sure that Power-On Self-Test (POST) is enabled.

If the problem persists, replace the switch.

BL-1027

Message: `Interface module in <slot string> faulted, boot failed; status 0x<boot status> 0x<1250 0 boot status> 0x<1250 1 boot status>`

Message Type: LOG

Severity: CRITICAL

Probable Cause: Indicates that the interface module failed to boot properly.

Recommended Action: Reload or power cycle the interface module using the **`power-off`** and **`power-on`** commands. If the message persists, replace the interface module.

BL-1028

Message: `Switch faulted; internal processor was reset before switch init completed.`

Message Type: LOG

Severity: CRITICAL

Probable Cause: Indicates that the switch internal processor was reset before the initialization completed.

Recommended Action: Reload or power cycle the switch. 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

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 data path elements were reset.

Recommended Action: No action is required.

BL-1031

Message: `Link timeout in internal port (slot number>, port <port number>) caused interface module fault. Use power-off/power-on commands to recover it.`

Message Type: LOG

Severity: CRITICAL

Probable Cause: Indicates that link timeout occurred in one of the back-end internal ports.

Recommended Action: Power cycle the interface module using the **`power-off`** and **`power-on`** commands.

BL-1032

Message: `(<slot string>,bitmap 0x<object control flags(bitmap)>) ports never came up ONLINE (reason <reason for port disable>, state <status of the interface module>). Disabling slot.`

Message Type: LOG

Severity: CRITICAL

Probable Cause: Indicates that the back-end (non-user) ports have not come online within the time limit.

Recommended Action: Reload or power cycle the interface module using the **`power-off`** and **`power-on`** commands.

Execute the **diag systemverification** command to verify that the interface module does not have hardware problems.

Execute the **diag post** command to make sure that Power-On Self-Test (POST) is enabled.

If the message persists, replace the interface module.

BL-1033

Message: `(<slot string>,bitmap 0x<object control flags(bitmap)>) No disable acknowledgment from ports (state <status of the interface module>). Disabling slot.`

Message Type: LOG

Severity: CRITICAL

Probable Cause: Indicates that the system has timed out waiting for the disable acknowledgment messages from the user ports.

Recommended Action: Reload or power cycle the interface module using the **power-off** and **power-on** commands.

Execute the **diag systemverification** command to verify that the interface module does not have hardware problems.

Execute the **diag post** command to make sure that Power-On Self-Test (POST) is enabled.

If the message persists, replace the interface module.

BL-1034

Message: `<slot string> CEE initialization completed.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that the specified slot has completed initializing the Converged Enhanced Ethernet (CEE) ports.

Recommended Action: No action is required.

BL-1037

Message: `Faulting chip in <slot string>, miniS = <mini-switch number>,port = <port number> due to BE/BI port fault.`

Message Type: LOG

Severity: CRITICAL

Probable Cause: Indicates that all ports on the chip have been disabled due to a fault on the chip.

Recommended Action: Execute the **diag systemverification** command to determine if there is a hardware error.

Execute the **diag post** command to make sure that Power-On Self-Test (POST) is enabled.

BL-1038

Message: `Inconsistent FPGA image version detected, reload the switch for recovery.`

Message Type: LOG

Severity: CRITICAL

Probable Cause: Indicates that the field-programmable gate array (FPGA) image version is incompatible with the software version.

Recommended Action: Reload the switch. If the message persists, replace the switch.

BL-1039

Message: `Inconsistent FPGA image version detected, faulting the interface module in <slot string>.`

Message Type: LOG

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 interface module using the **power-off** and **power-on** commands. If the message persists, replace the interface module.

BL-1045

Message: `mini SFP+ (SN: <mini SFP+ serial number>) is only supported in certain high port count interface modules, not interface module in <slot number of interface module that has the mini SFP+> with ID <Interface module ID of interface module that has the mini SFP+ that does not support it>`

Message Type: LOG

Severity: ERROR

Probable Cause: Indicates that the mini (form factor) enhanced small form-factor pluggable (SFP+) transceiver is supported only by a certain type of interface module, but it can be inserted in other interface modules.

Recommended Action: Replace the mini SFP+ transceiver with an SFP or SFP+ transceiver.

BL-1046

Message: `<slot number of interface module 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>). Reseat or replace the SFP.`

Message Type: LOG

Severity: ERROR

Probable Cause: Indicates that 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 number>.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that the buffer optimized mode is changed for the specified slot chassis.

Recommended Action: No action is required.

BL-1049

Message: `Incompatibility with an active 12x40G LC detected, faulting the interface module in <slot string>.`

Message Type: LOG

Severity: CRITICAL

Probable Cause: Indicates that this line card (LC) is incompatible with one or more existing 12x40G LCs.

Recommended Action: Power cycle all active 12X40G LCs and then power cycle the interface module using the **power-off** and **power-on** commands. Then power on all 12X40G LCs. After completing these steps, all LCs can interoperate with one another.

BL-1050

Message: `Media is not supported on this platform (slot <slot number>, port <port number>).`

Message Type: LOG

Severity: ERROR

Probable Cause: Indicates that the media on the specified port is bad or incompatible with this platform.

Recommended Action: Replace a different media on the specified port.

BL-1051

Message: `The media is not verified for this platform (slot <slot number>, port <port number>).`

Message Type: LOG

Severity: WARNING

Probable Cause: Indicates that the media on the specified port is not verified with this platform.

Recommended Action: Extreme recommends to use a supported media on this platform. You can still use an unsupported media at your own risk.

BL-1052

Message: `<slot NIF init failed. Code:<result>.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that linecard NIF init failed.

Recommended Action: No action is required.

BLL Messages

BLL-1000

Message: `ASIC driver detected <slot string> port <port number> as faulty (reason: <reason code>).`

Message Type: FFDC | LOG

Severity: CRITICAL

Probable Cause: Indicates that an interface module regulation problem was reported on the specified slot. The interface module is faulted.

The reason codes are as follows:

1 = Available buffer overflow

2 = Backend port buffer timeout

3 = Backend port got shut down

4 = Embedded port buffer timeout

5 = Excessive busy mini buffer

6 = Excessive RCC VC on E_Port

7 = Excessive RCC VC on FL_Port

8 = Fail detection buffer tag error

9 = Fail detection TX parity error

10 = EPI CMEM interrupt error

11 = Checkpoint Middleware Interface (CMI) interrupt error

12 = Interrupt overrun

13 = FDET interrupt

14 = Interrupt suspended

15 = Filter LISTD error

16 = Unknown filter LIST error

17 = Wait for LPC open state

18 = Wait for Old port state

19 = Wait for Open init state

20 = TX parity error

21 = RAM parity error

22 = Built in Self Repair (BISR) or RAMINIT error

Recommended Action:

Make sure the interface module is seated correctly. If the interface module is seated correctly, reload or power cycle the interface module using the **power-off** and **power-on** commands.

Execute the **diag systemverification** command to verify that the interface module does not have hardware problems.

If the message persists, replace the interface module.

CHS Messages

CHS-1002

Message: `ki_gd_register_action failed with rc = <return value>.`

Message Type: LOG | FFDC

Severity: ERROR

Probable Cause: Indicates an internal error

Recommended Action: Reload or power cycle the switch

CHS-1003

Message: `Slot ENABLED but Not Ready during recovery, disabling slot = <slot number>, rval = <return value>.`

Message Type: LOG

Severity: ERROR

Probable Cause: Indicates that the slot state has been detected as inconsistent during or recovery.

Recommended Action: For a modular switch, execute the **power-off** and **power-on** commands to power cycle the interface module.

For a compact switch, reload or power cycle the switch.

CHS-1004

Message: `Interface module attach failed during recovery, disabling slot = <slot number>, rval = <return value>.`

Message Type: LOG

Severity: ERROR

Probable Cause: Indicates that the specified interface module has failed during or recovery.

Recommended Action: For a modular switch, execute the **power-off** and **power-on** commands to power cycle the interface module.

For a compact switch, reload or power cycle the switch.

CHS-1005

Message: `Diag attach failed during recovery, disabling slot = <slot number>.`

Message Type: LOG

Severity: ERROR

Probable Cause: Indicates that the diagnostic interface module attach operation has failed during or recovery.

Recommended Action: For a modular switch, execute the **power-off** and **power-on** commands to power cycle the interface module.

For a compact switch, reload or power cycle the switch.

DAD Messages

DAD-1300

Message: `DHCP Auto-Deployment firmware download start.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that DHCP automatic firmware download has started.

Recommended Action: No action is required.

DAD-1301

Message:`DHCP Auto-Deployment failed due to dual-MM HA sync timeout.`

Message Type: AUDIT | LOG

Severity: ERROR

Probable Cause: Indicates that the DHCP Auto Deployment (DAD) process has failed because HA synchronization of the dual-management module has timed out.

Recommended Action: No action is required.

DAD-1302

Message: `DHCP Auto-Deployment failed during DHCP process.`

Message Type: LOG

Severity: ERROR

Probable Cause: Indicates that the DHCP Auto Deployment (DAD) process failed because the dhclient is not getting the FTP server IP or the firmware path information.

Recommended Action: No action is required.

DAD-1303

Message: `Last firmware download session is in progress.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that the previous firmware download session is still in progress.

Recommended Action: No action is required.

DAD-1304

Message: `Last firmware download session failed.`

Message Type: LOG

Severity: ERROR

Probable Cause: Indicates that the last firmware download session has failed.

Recommended Action: No action is required.

DAD-1305

Message: `DHCP Auto-Deployment cluster formation timeout.`

Message Type: LOG

Severity: ERROR

Probable Cause: Indicates that not all nodes have completed DHCP Auto Deployment (DAD) before the current DAD session limit.

Recommended Action: No action is required.

DAD-1306

Message: `DHCP Auto-Deployment sanity check failed.`

Message Type: LOG

Severity: ERROR

Probable Cause: Indicates that the DHCP Auto Deployment (DAD) sanity check has failed.

Recommended Action: No action is required.

DAD-1307

Message: `DHCP Auto-Deployment principle node ready.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that the principle node is ready for the secondary node to join.

Recommended Action: No action is required.

DAD-1308

Message: `Current firmware skip firmware download.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that the new firmware is already loaded on the switch and therefore there is no need to trigger firmware download.

Recommended Action: No action is required.

DAD-1309

Message: `DHCP Auto-Deployment session fail to start firmware download.`

Message Type: LOG

Severity: ERROR

Probable Cause: Indicates that the DHCP Auto Deployment (DAD) session has failed to start firmware download.

Recommended Action: No action is required.

DAD-1310

Message: `DHCP Auto-Deployment firmware download completed successfully.`

Message Type: AUDIT | LOG

Severity: INFO

Probable Cause: Indicates that the DHCP Auto Deployment (DAD) process has completed successfully.

Recommended Action: No action is required.

DAD-1311

Message: `DHCP Auto-Deployment firmware download failed.`

Message Type: AUDIT | LOG

Severity: ERROR

Probable Cause: Indicates that the DHCP Auto Deployment (DAD) process has failed.

Recommended Action: No action is required.

DAD-1312

Message: `DHCP Auto-Deployment node succeeded.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that DHCP Auto Deployment (DAD) succeeded on the node.

Recommended Action: No action is required.

DAD-1313

Message: `DHCP Auto-Deployment cluster partially succeeded.`

Message Type: LOG

Severity:WARNING

Probable Cause: Indicates that some of the nodes are not in the cluster before the DHCP Auto Deployment (DAD) session time limit.

Recommended Action: No action is required.

DAD-1314

Message: `DHCP Auto-Deployment cluster succeeded.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that DHCP Auto Deployment (DAD) succeeded on all nodes.

Recommended Action: No action is required.

DAD-1315

Message: `DHCP Auto-Deployment firmware mismatch.`

Message Type: LOG

Severity: WARNING

Probable Cause: Indicates that the secondary node has a different firmware from the principle node.

Recommended Action: No action is required.

DAD-1316

Message: `DHCP Auto-Deployment running global configuration script.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that DHCP Auto Deployment (DAD) is running global configuration script.

Recommended Action: No action is required.

DAD-1317

Message: `DHCP Auto-Deployment complete global configuration script`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that DHCP Auto Deployment (DAD) has completed running global configuration script.

Recommended Action: No action is required.

DAD-1318

Message: `DHCP Auto-Deployment running local configuration script.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that DHCP Auto Deployment (DAD) is running local configuration script.

Recommended Action: No action is required.

DAD-1319

Message: `DHCP Auto-Deployment complete local configuration script.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that DHCP Auto Deployment (DAD) has completed running local configuration script.

Recommended Action: No action is required.

DAD-1320

Message: `DHCP Auto-Deployment running local command.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that DHCP Auto Deployment (DAD) is running local command.

Recommended Action: No action is required.

DAD-1321

Message: `DHCP Auto-Deployment complete local command.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that DHCP Auto Deployment (DAD) has completed running local command.

Recommended Action: No action is required.

DAD-1322

Message: `DHCP Auto-Deployment unexpected switch reboot.`

Message Type: LOG

Severity: WARNING

Probable Cause: Indicates that an unexpected switch reboot has occurred in the middle of the DHCP Auto Deployment (DAD) session.

Recommended Action: No action is required.

DAD-1323

Message: `DHCP Auto-Deployment parameter error.`

Message Type: LOG

Severity: ERROR

Probable Cause: Indicates that a parameter (*/etc/fabos/dad/dadparams*) error has occurred.

Recommended Action: No action is required.

DAD-1324

Message: `DHCP Auto-Deployment wait for principle node timeout.`

Message Type: LOG

Severity: ERROR

Probable Cause: Indicates that the secondary node has not found the DHCP Auto Deployment (DAD) principle node in the cluster.

Recommended Action: No action is required.

DAD-1325

Message: `DHCP Auto-Deployment principle node in cluster is not in principle role.`

Message Type: LOG

Severity: ERROR

Probable Cause: Indicates that the secondary node has found the DHCP Auto Deployment (DAD) principle node in the cluster, but the principle node is not in principle role.

Recommended Action: No action is required.

DAD-1326

Message: `DHCP Auto-Deployment timeout when wait for CLI ready.`

Message Type: LOG

Severity: ERROR

Probable Cause: Indicates that the Network OS CLI has failed to start up

Recommended Action: No action is required.

DAD-1327

Message: `DHCP Auto-Deployment timeout when running local command.`

Message Type: LOG

Severity: ERROR

Probable Cause: Indicates that the local command was running for a long time.

Recommended Action: No action is required.

DAD-1328

Message: `DHCP Auto-Deployment secondary node timeout when joining cluster.`

Message Type: LOG

Severity: ERROR

Probable Cause: Indicates that the secondary node was taking long time to join the cluster.

Recommended Action: No action is required.

DAD-1329

Message: `DHCP Auto-Deployment fail to copy running-config startup-config.`

Message Type: LOG

Severity: ERROR

Probable Cause: Indicates that DHCP Auto Deployment (DAD) has failed to copy the running configuration to the startup configuration.

Recommended Action: No action is required.

DAD-1330

Message: `DHCP Auto-Deployment secondary node fail to notify principle node.`

Message Type: LOG

Severity: ERROR

Probable Cause: Indicates that the secondary node has failed to send update to the principle node.

Recommended Action: No action is required.

DAD-1340

Message: `DHCP Auto-Deployment succeed to download option 239 script.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that the option 239 script is downloaded.

Recommended Action: No action is required.

DAD-1341

Message: `DHCP Auto-Deployment starts option 239 script.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that the option 239 script starts to run.

Recommended Action: No action is required.

DAD-1342

Message: `XMC Discovery Succeed`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that Cloud Connector Discovery Succeed.

Recommended Action: No action is required.

DCM Messages

DCM-1002

Message:`PostBoot processing on <Configuration name> has started.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that the PostBoot processing on the specified configuration group has started.

Recommended Action: No action is required.

DCM-1003

Message:`PostBoot processing on <Configuration name> is complete.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that the PostBoot processing on the specified configuration group has been completed.

Recommended Action: No action is required.

DCM-1004

Message: `Configuration File Replay has started.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that the configuration replay has started.

Recommended Action: No action is required.

DCM-1005

Message: `Configuration Replay is complete.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that the configuration replay has been completed.

Recommended Action: No action is required.

DCM-1006

Message: `Event: <Event Name>, Status: <Command status>, User command: <ConfD hpath string>.`

Message Type: AUDIT

Class: DCMCFG

Severity: INFO

Probable Cause: Indicates that the user command has been executed successfully.

Recommended Action: No action is required.

DCM-1007

Message: `No Configuration File Replay.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that configuration file replay will not happen on this system boot up.

Recommended Action: No action is required.

DCM-1008

Message: `Configuration has been reset to default due to changes in configuration metadata.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that the configuration schema has changed and therefore the old configuration cannot be retained.

Recommended Action: Replay the saved configuration manually.

DCM-1013

Message: `Reset terminal timeout: <Timeout Reset Command>.`

Message Type: AUDIT

Class: DCMCFG

Severity: INFO

Probable Cause: Indicates that terminal timeout has been reset.

Recommended Action: No action is required.

DCM-1014

Message: `Error Node replace model mismatch, chassis disabled WWN: <switch_wwn>.`

Message Type: AUDIT | LOG

Severity: ERROR

Probable Cause: Indicates that the replacement switch model is different from the model of switch being replaced; this is not supported and therefore the chassis has been disabled.

Recommended Action: Use the same switch model for replacement.

DCM-1015

Message: `Switch is prepared for power-cycle. No clis will work henceforth. Need power-cycle or reload to make switch fully functional.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that database is shutdown gracefully so that node is power-cycle ready.

Recommended Action: Power-cycle or Reload to make switch fully functional.

DCM-1016

Message: `Switch is in ZTP mode. Configuration related commands will not be allowed. Cancel ZTP or wait until ZTP has completed to make changes to the switch configuration.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that ZTP mode is enabled and configuration related commands will not be allowed.

Recommended Action: Cancel ZTP mode or wait untl ZTP has completed to make changes to the switch configuration.

DCM-1101

Message: `Copy running-config to startup-config operation successful on this node.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that the running configuration has been copied to the startup configuration on the node.

Recommended Action: No action is required.

DCM-1102

Message: `Copy running-config to startup-config operation failed on this node.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates failure to copy the running configuration to the startup configuration on the node.

Recommended Action: No action is required.

DCM-1103

Message: `Copy default-config to startup-config operation successful on this node.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that the default configuration has been copied to the startup configuration on the node.

Recommended Action: No action is required.

DCM-1104

Message: `Copy default-config to startup-config operation failed on this node.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates failure to copy the default configuration to the startup configuration on the node.

Recommended Action: No action is required.

DCM-1105

Message: `Copy of the downloaded config file to the current running-config has completed successfully on this node.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that the downloaded configuration file has been copied to the current running configuration.

Recommended Action: No action is required.

DCM-1106

Message: `Copy of the downloaded config file to the current startup-config has completed successfully on this node.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that the downloaded configuration file has been copied to the current startup configuration.

Recommended Action: No action is required.

DCM-1107

Message: `Startup configuration file has been uploaded successfully to the remote location.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that the startup configuration file has been uploaded successfully.

Recommended Action: No action is required.

DCM-1108

Message: `Running configuration file has been uploaded successfully to the remote location.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that the running configuration file has been uploaded successfully.

Recommended Action: No action is required.

DCM-1109

Message: `Error (<error string>) encountered while copying configuration to flash/USB.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates a failure to copy configuration file to flash or USB storage device.

Recommended Action: No action is required.

DCM-1110

Message: `Last configuration replay complete.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that a configuration was in progress during high availability and the configuration has been replayed.

Recommended Action: No action is required.

DCM-1111

Message: `Error (<error string>) last configuration replay failed.`

Message Type: LOG

Severity: ERROR

Probable Cause: Indicates that a configuration was in progress during high availability and the configuration replay has failed.

Recommended Action: Reconfigure the failed command.

DCM-1112

Message: `Running configuration file has been uploaded successfully to flash.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that the running configuration file has been uploaded successfully.

Recommended Action: No action is required.

DCM-1113

Message: `Running configuration file has been uploaded successfully to USB.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that the running configuration file has been uploaded successfully to a USB storage device.

Recommended Action: No action is required.

DCM-1114

Message: `Startup configuration file has been uploaded successfully to flash.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that the startup configuration file has been uploaded successfully.

Recommended Action: No action is required.

DCM-1115

Message: `Startup configuration file has been uploaded successfully to USB.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that the startup configuration file has been uploaded successfully.

Recommended Action: No action is required.

DCM-1116

Message: `System initialization is complete. SLX-OS is ready to handle all commands.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that SLX-OS is ready to handle all commands after system initialization completion.

Recommended Action: No action is required.

DCM-1117

Message: `File has been uploaded successfully to USB.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that file has been uploaded successfully to USB.

Recommended Action: No action is required.

DCM-1118

Message: `Error while transferring file over tftp. Reason: <error string>`

Message Type: LOG

Severity: ERROR

Probable Cause: Indicates a failure while transferring file over tftp.

Recommended Action: Refer to the reason code indicated in the command output for possible action.

DCM-1119

Message: `Copy file from flash completed successfully`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates a successful copy of file from flash.

Recommended Action: No action is required.

DCM-1120

Message: `Error while copying file from flash. Reason: <error string>`

Message Type: LOG

Severity: ERROR

Probable Cause: Indicates a failure while copying file from flash.

Recommended Action: Refer to the reason code indicated in the command output for possible action.

DCM-1123

Message: `Configuration Rollback to checkpoint <Checkpoint Name> has started.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that the configuration rollback has started.

Recommended Action: No action is required.

DCM-1124

Message: `Configuration Rollback to checkpoint <Checkpoint Name> has been completed successfully.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that the configuration rollback has been completed successfully.

Recommended Action: No action is required.

DCM-1125

Message: `Configuration Rollback to checkpoint <Checkpoint Name> has been completed partially.`

Message Type: LOG

Severity: ERROR

Probable Cause: Indicates that the configuration rollback has been completed partially.

Recommended Action: No action is required.

DCM-1126

Message: `Configuration Rollback to checkpoint <Checkpoint Name> has failed.`

Message Type: LOG

Severity: ERROR

Probable Cause: Indicates failure to perform configuration rollback to the specified checkpoint.

Recommended Action: No action is required.

DCM-1127

Message: `Configuration Rollback to checkpoint <Checkpoint Name> is aborted.`

Message Type: LOG

Severity: ERROR

Probable Cause: Indicates that the configuration rollback to the specified checkpoint is aborted.

Recommended Action: No action is required.

DCM-1128

Message: `Checkpoint <Checkpoint Name> is created by user <User Name>`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that the checkpoint is created successfully.

Recommended Action: No action is required.

DCM-1129

Message: `Checkpoint <Checkpoint Name> is Deleted by user <User Name>`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that the checkpoint is deleted successfully.

Recommended Action: No action is required.

DCM-1201

Message: `FIPS Zeroize operation request received.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that the Federal Information Protection Standard (FIPS) Zeroize operation request has been received.

Recommended Action: No action is required.

DCM-1204

Message: `FIPS Zeroize operation: all client sessions are notified that Zeroize in progress.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that all client sessions are notified about the Federal Information Protection Standard (FIPS) Zeroize operation in progress and the commands cannot be executed.

Recommended Action: No action is required.

DCM-1205

Message: `FIPS Zeroize operation: starting with cleanup for Zeroize.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that the configuration files cleanup for Federal Information Protection Standard (FIPS) Zeroize has started.

Recommended Action: No action is required.

DCM-1206

Message: `FIPS Zeroize operation: starting prepare phase for Zeroize.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that the prepare phase for Federal Information Protection Standard (FIPS) Zeroize has started, during which all the services will be shut down.

Recommended Action: No action is required.

DCM-1207

Message: `FIPS Zeroize operation: failed in prepare phase step for Zeroize.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that the Federal Information Protection Standard (FIPS) Zeroize operation has failed during the prepare phase.

Recommended Action: No action is required.

DCM-1208

Message: `FIPS Zeroize operation: Running Zeroize for secure deletion of the user configuration data.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that the Federal Information Protection Standard (FIPS) Zeroize operation is running for secure deletion of the user configuration data.

Recommended Action: No action is required.

DCM-1209

Message: `FIPS Zeroize operation: failed during secure deletion of the user configuration data.`

Message Type: LOG

Severity: ERROR

Probable Cause: Indicates that the Federal Information Protection Standard (FIPS) Zeroize operation has failed during secure deletion of the user configuration data.

Recommended Action: Refer to the reason code indicated in the **`fips zeroize`** command output for possible action.

DCM-1210

Message: `FIPS Zeroize operation failed.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that the Federal Information Protection Standard (FIPS) Zeroize operation has failed.

Recommended Action: No action is required.

DCM-1211

Message: `FIPS Zeroize operation executed successfully.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that the Federal Information Protection Standard (FIPS) Zeroize operation has been executed successfully.

Recommended Action: No action is required.

DCM-1212

Message: `FIPS Zeroize operation failed. Node zeroizing or already zeroized.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that the Federal Information Protection Standard (FIPS) Zeroize operation has failed because the node is zeroizing or it was already zeroized.

Recommended Action: No action is required.

DCM-1301

Message: `Bare-Metal state is <Bare-Metal state>.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates if the switch is in the bare-metal state.

Recommended Action: No action is required.

DCM-1401

Message: `Event-Handler: Exclusive run-mode action has been triggered and is active. Cluster formation operations will be paused.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that an activated event-handler that is configured with exclusive run-mode has been triggered. Cluster formation operations will be paused.

Recommended Action: No action is required.

DCM-1402

Message: `Event-Handler: Exclusive run-mode action has completed and is inactive. Cluster formation operations will be resumed.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that an activated event-handler that is configured with exclusive run-mode has completed. Cluster formation operations will be resumed.

Recommended Action: No action is required.

DCM-1403

Message: `Event-Handler: Action execution (Event-Handler: <Event-Handler Name>, Action Script: <Action Script Name>) timed out.`

Message Type: LOG

Severity: ERROR

Probable Cause: Indicates that the action script associated with one of the event-handlers timed out.

Recommended Action: In case action script is going to take longer, reconfigure the event-handler activation action-timeout to a higher value.

DCM-1457

Message: `At {upgrade/install-stage} stage, detected default password being used for default TPVM user 'extreme'. Set password under TPVM Config.`

Message Type: LOG

Severity: INFO

Probable Cause: Default password detected for the default TPVM user during the TPVM upgrade process. The current stage of the upgrade is shown in the message.

Recommended Action: Change the password for the default TPVM user as soon as possible.

DCM-1458

Message: `Aborting TPVM upgrade. Default password used for TPVM user 'extreme'. Set password under TPVM config.`

Message Type: LOG

Severity: ERROR

Probable Cause: Default password is configured for the default TPVM user for the existing TPVM instance. This was detected during the TPVM upgrade process.

Recommended Action: Change the password for the default TPVM user before restating the upgrade.

DCM-1471

Message: `BMC set <operation> <enqueue-count>scheduled`

Message Type: LOG

Severity: INFO

Probable Cause: Schedule (Enqueue) of an <Operation Name> by CLI/REST with enqueue count.

Recommended Action: No action is required.

DCM-1472

Message: `BMC set <operation> <enqueue-count> at backend kickstarted.`

Message Type: LOG

Severity: INFO

Probable Cause: Enqueued operation <operation> with <enqueue-count> is started at the backend.

Recommended Action: No action is required.

DCM-1473

Message: `BMC set <operation> <enqueue-count> completed successfully`

Message Type: LOG

Severity: INFO

Probable Cause: Enqueued operation <operation> with <enqueue-count> has completed successfully at the backend.

Recommended Action: No action is required.

DCM-1474

Message: `BMC set <operation> <enqueue- count> failed. Reason:<error-reason>. Hint:<error-hint>`

Message Type: LOG

Severity: ERROR

Probable Cause: Reason can be found in <error-reason>

Recommended Action: Probable action can be based on <error-hint>.

DCM-1475

Message: `BMC config autopopulated from BMC oper data as one time post upgrade activity from <bmc-version-from> to <bmc-version-to>`

Message Type: LOG

Severity: INFO

Probable Cause: BMC configuration is autopopulated from *BMC oper data* as a one time post upgrade activity from the specified BMC from version to the specified BMC to version.

Recommended Action: No action is required.

DCM-2001

Message: `Event: <Event Name>, Status: success, Info: Successful login attempt through <connection method and IP Address>.`

Message Type: AUDIT

Class: DCMCFG

Severity: INFO

Probable Cause: Indicates that the log in was successful. An IP address is displayed when the login occurs over a remote connection.

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.

DCM-2002

Message: `Event: <Event Name>, Status: success, Info: Successful logout by user [<User>].`

Message Type: AUDIT

Class: DCMCFG

Severity: INFO

Probable Cause: Indicates that the specified user has successfully logged out.

Recommended Action: No action is required.

DCM-3005

Message: `Software assert error detected in configuration manager service: <message>.`

Message Type: LOG | FFDC

Severity: ERROR

Probable Cause: Indicates an error condition hit by the configuration manager (DCM) caused ASSERT.

Recommended Action: Execute the **`copy support`** command and contact your switch service provider.

DCM-3010

Message: <Database Name> database integrity check timed out after <Timeout in minutes> minutes.

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that the database integrity check timeout has occurred.

Recommended Action: No action is required.

DCM-3051

Message: `Encountered Database Corruption. System going down for auto-recovery.`

Message Type: LOG

Severity: ERROR

Probable Cause: Indicates that the database operation failed because of database corruption. The system reloads for auto-recovery of the database.

Recommended Action: No action is required.

DCM-3052

Message: `Database Corruption was detected. Therefore, system was rebooted for recovery and may have taken longer than usual.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that the last system reload was for auto-recovery of database because the database corruption was detected.

Recommended Action: No action is required.

DCM-3053

Message: <Database name> database corruption was detected. The system will startup with the default configuration for this database.

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that database corruption was detected. The system has auto-recovered with the default configuration applied.

Recommended Action: No action is required.

DCM-3054

Message: `Event: Client <IP> is connected to telemetry server.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that a client is connected to telemetry server.

Recommended Action: No action is required.

DCM-3055

Message: `Event: Client <IP> is disconnected from telemetry server.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that a client is disconnected from telemetry server.

Recommended Action: No action is required.

DCM-3056

Message: `Event: Max limit on clients connected to telemetry server reached.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that a max number of clients connected to telemetry server.

Recommended Action: No action is required.

DCM-3100

Message: `Event: Connection to collector <Collector Name> has been established.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that a collector connection has been established.

Recommended Action: No action is required.

DCM-3101

Message: `Event: Collector <Collector Name> has been disconnected.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that a collector has been disconnected.

Recommended Action: No action is required.

DCM-4001

Message: `Database schema conversion succeeded.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that after a firmware download, the database schema was successfully converted to the schema supported by the firmware.

Recommended Action: No action is required.

DCM-4002

Message: `Database schema conversion failed.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that after a firmware download, a failure was encountered in converting the database schema to the schema supported by the firmware.

Recommended Action: No action is required.

DOT1 Messages

DOT1-1001

Message: `802.1X is enabled globally.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that 802.1X is enabled globally.

Recommended Action: No action is required.

DOT1-1002

Message:`802.1X is disabled globally.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that 802.1X is disabled globally

Recommended Action: No action is required.

DOT1-1003

Message: `802.1X is enabled for interface <port_name>.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that 802.1X is enabled on the specified interface.

Recommended Action: No action is required.

DOT1-1004

Message: `interface <port_name> is forcefully unauthorized.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that the specified interface has been unauthorized forcefully using the <cmd>dot1x port-control force-unauthorized</cmd> command.

Recommended Action: No action is required.

DOT1-1005

Message: `802.1X authentication is successful on interface <port_name>.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that authentication has succeeded on the specified interface.

Recommended Action: No action is required.

DOT1-1006

Message: `802.1X authentication has failed on interface <port_name>.`

Message Type: DCE

Severity: WARNING

Probable Cause: Indicates that authentication has failed on the specified interface due to incorrect credentials or the remote authentication dial-in user service (RADIUS) server is not functioning properly.

Recommended Action: Check the credentials configured with the supplicant and RADIUS server. You can reconfigure the attributes on the RADIUS server using the **`radius-server`** command.

DOT1-1007

Message: `No RADIUS server available for authentication.`

Message Type: DCE

Severity: CRITICAL

Probable Cause: Indicates that there is no remote authentication dial-in user service (RADIUS) server available for authentication.

Recommended Action: Check whether the configured RADIUS servers are reachable and are functioning.

DOT1-1008

Message: `interface <port_name> is forcefully authorized.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that the specified interface has been authorized forcefully using the **`dot1x port-control forced-authorized`** command.

Recommended Action: No action is required.

DOT1-1009

Message: `802.1X is disabled for interface <port_name>.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that 802.1X is disabled on the specified interface.

Recommended Action: No action is required.

DOT1-1010

Message: `interface <port_name> is set in auto mode.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that the specified interface is set to auto mode.

Recommended Action: No action is required.

DOT1-1011

Message: `DOT1X_PORT_EAPOL_CAPABLE: Peer with MAC <mac1><mac2>.<mac3><mac4>.<mac5><mac6> connected to interface <port_name> is EAPOL Capable`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that the peer connected to the specified interface is DOT1X-capable.

Recommended Action: No action is required.

DOT1-1012

Message: `DOT1X_PORT_EAPOL_CAPABLE: Peer connected to interface <port_name> is NOT EAPOL capable.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that the peer connected to the specified interface is not DOT1X-capable.

Recommended Action: No action is required.

DOT1-1013

Message: `DOT1X test timeout value is set to <Updated test timeout value>.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that the DOT1X test timeout value has been changed to the specified value.

Recommended Action: No action is required.

DOT1-1014

Message: `DOT1X Radius Dynamic VLAN assignment failure. Missing Radius attribute(s) TunnelType / TunnelMediumType for interface <port_name> user: <User Name>.`

Message Type: DCE

Severity: ERROR

Probable Cause: Indicates that the DOT1X required Radius attribute(s) is/are missing.

Recommended Action: Include both Radius attributes TunnelType and TunnelMediumType along with attribute PrivateGroupId in the Radius Server.

DOT1-1014

Message: `DOT1X Radius Dynamic VLAN assignment failure. Missing Radius attribute(s) TunnelType / TunnelMediumType for interface <port_name> user: <User Name>.`

Message Type: DCE

Severity: ERROR

Probable Cause: Indicates that the DOT1X required Radius attribute(s) is/are missing.

Recommended Action: Include both Radius attributes TunnelType and TunnelMediumType along with attribute PrivateGroupId in the Radius Server.

DOT1-1015

Message: `Access port is already associated with VLAN assigned by Radius.`

Message Type: DCE

Severity: INFO

Probable Cause: Access port is already assigned with VLAN.

Recommended Action: No action is required.

ELD Messages

ELD-1001

Message:`interface <InterfaceName> is shut down by loop detection (LD)<VLAN ID>`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that a loop has been detected by the loop detection (LD) protocol on the specified interface. The interface has been shut down.

Recommended Action: Identify and fix the Layer 2 bridging loop and then re-enable the interface using the **`clear loop-detection`** command.

ELD-1002

Message: `interface <InterfaceName> is auto-enabled by loop detection (LD).`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that the interface on which a loop was detected has been auto-enabled based on the configured shutdown time.

Recommended Action: No action is required.

ELD-1003

Message: `Loop detected on interface <InterfaceName> vlan <VLAN ID> and no shut down due to shut-down-disabled by loop detection (LD).`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that a loop has been detected by the loop detection (LD) protocol on the specified interface. The interface is not been shut down due to shut-down-disabled (LD) configured on interface.

Recommended Action: loop has been detected and no interface shutdown performed. Check LD shut-down-disabled command under interface.

ELD-1004

Message: `Loop detected on MCT vlan <VLAN ID> enable loop detection for the VLAN on the peer cluster node.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that a loop has been detected by the loop detection (LD) for MCT VLAN. The interface is not shut down as its used of MCT peer communication.

Recommended Action: Loop has been detected and no interface shutdown performed. Check LD is enabled on the peer MCT node for this VLAN.

ELD-1005

Message: `Loop is detected on <InterfaceName> <VLAN ID>, the LIF (logical interface) is shutdown.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that a loop has been detected by the loop detection (LD) protocol on the specified interface.

Recommended Action: loop has been detected and shutdown the LIF.

ELD-1006

Message: `Loop is detected on <InterfaceName> <VLAN ID>, but shutdown action is not performed due to shutdown action is disabled.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that a loop has been detected by the loop detection (LD) protocol on the specified interface.

Recommended Action: do nothing because LIF LD shutdown is disabled.

ELD-1007

Message: `Loop detection disabled LIF (Logical interface) on <InterfaceName> <VLAN ID> is <HowTo>-enabled.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that the interface on which a loop was detected has been auto-enabled based on the configured shutdown time.

Recommended Action: No action is required.

ELD-1008

Message: `Loop is detected on VxLAN <InterfaceName> <VNI> <VLAN ID>, the LIF (logical interface) is shutdown.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that a loop has been detected by the loop detection (LD) protocol on the specified interface.

Recommended Action: loop has been detected and shutdown the LIF.

ELD-1009

Message: `Loop is detected on VxLAN <InterfaceName> <VNI> <VLAN ID>, but shutdown action is not performed due to shutdown action is disabled.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that a loop has been detected by the loop detection (LD) protocol on the specified interface.

Recommended Action: do nothing because LIF LD shutdown is disabled.

ELD-1010

Message: `Loop detection disabled LIF (Logical interface) on VxLAN <InterfaceName> <VNI> <VLAN ID> is <HowTo>-enabled.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that the interface on which a loop was detected has been auto-enabled based on the configured shutdown time.

Recommended Action: No action is required.

ELD-1011

Message: `VxLAN LIF (logical interface) on VxLAN <InterfaceName> <VNI> <VLAN ID> is shutdown by Loop Detection.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that a loop has been detected by the loop detection (LD) protocol, and the VxLAN LIF is shutdown because of it.

Recommended Action: loop has been detected and shutdown the LIF.

EM Messages

EM-1001

Message: `<FRU ID> is overheating: Shutting down.`

Message Type: FFDC | LOG

Severity: CRITICAL

Probable Cause: Indicates that a field replaceable unit (FRU) is shutting down due to overheating. Overheating is mainly 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.

Execute the **`show environment fan`** command to verify that all fans are running at normal speeds. Replace fans that are missing or not performing at high enough speeds.

EM-1002

Message:`System fan(s) status <fan FRU>.`

Message Type: LOG | FFDC

Severity: INFO

Probable Cause: Indicates that a compact system has overheated and may shut down. All the fan speeds are dumped to the console.

Recommended Action: Verify that the location temperature is within the operational range of the switch.

Execute the **`show environment fan`** command to verify that all fans are running at normal speeds. Replace fans that are missing or not performing at high enough speeds.

EM-1003

Message: `<FRU ID> has unknown hardware identifier: FRU faulted.`

Message Type: FFDC | LOG

Severity: CRITICAL

Probable Cause: Indicates that a field-replaceable unit (FRU) header cannot be read or is invalid. The FRU is faulted.

Recommended Action: Reload or power cycle the switch.

Execute the **`diag systemverification`** command to verify that the switch does not have hardware problems

EM-1004

Message: `<FRU ID> failed to power on.`

Message Type: FFDC | LOG

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 a FRU type string and an optional number to identify the unit, slot, or port.

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

Severity: CRITICAL

Probable Cause: Indicates that an interface module in the specified slot or the switch (for compact switches) is being shut down for environmental reasons; its temperature or voltage is out of range.

Recommended Action: Check the environment and make sure the room temperature is within the operational range of the switch. Execute the **`show environment fan`** command to verify fans are operating properly. Make sure there are no blockages of the airflow around the chassis. If the temperature problem is isolated to the interface module itself, replace the interface module.

Voltage problems on a interface module are likely a hardware problem on the interface module itself; replace the interface module.

EM-1006

Message: `<FRU Id> has faulted. Sensor(s) below minimum limits.`

Message Type: FFDC | LOG

Severity: CRITICAL

Probable Cause: Indicates that the sensors show the voltage is below minimum limits. The switch or specified interface module is being shut down for environmental reasons; the voltage is too low.

Recommended Action: If this problem occurs on an interface module, it usually indicates a hardware problem on the interface module; replace the interface module.

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 firmware version as a possible cause.`

Message Type: FFDC | LOG

Severity: CRITICAL

Probable Cause: Indicates that an interface module inserted in the specified slot or the switch (for compact switches) is not compatible with the platform configuration (includes the firmware version). The interface module is faulted.

Recommended Action: If the interface module is not compatible, upgrade the firmware or replace the interface module and make sure the replacement interface module is compatible with your management module type and firmware.

EM-1009

Message: `<FRU Id> powered down unexpectedly.`

Message Type: FFDC | LOG

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

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 4 seconds.

Recommended Action: Reseat the interface module. If the problem persists, replace the interface module.

EM-1011

Message: `Received unexpected power down for <FRU Id>, but cannot determine if it has power.`

Message Type: FFDC | LOG

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 4 seconds it could not be determined if it has powered down or not.

Recommended Action: Reseat the interface module. If the problem persists, replace the interface module.

EM-1012

Message: `<FRU Id> failed <state> state transition, unit faulted.`

Message Type: FFDC | LOG

Severity: CRITICAL

Probable Cause: Indicates that a switch interface module or compact 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 Network OS configuration or hardware problems on the switch.

Recommended Action: Reload or power cycle the switch.

Execute the **`diag systemverification`** command to verify that the switch does not have hardware problems.

EM-1013

Message: `Failed to update FRU information for <FRU Id>.`

Message Type: LOG

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 an field-replaceable unit (FRU.

Recommended Action: 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

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

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, reload or power cycle the switch.

EM-1016

Message: `Cold recovery failed (<Return code>).`

Message Type: LOG

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 message persists, execute the **copy support** command and contact your switch service provider.

EM-1020

Message: `A problem was found on one or both CID cards (<The return code is for internal use only.>), run the CIDrecov tool to get more information and recovery options.`

Message Type: LOG

Severity: ERROR

Probable Cause: Indicates that a problem was found either accessing one (or both) of the CID 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 CID cards.

Recommended Action: Execute the **CIDrecov** command to get details of the problems found and how to recover.

EM-1021

Message: `A CID card has been inserted, a CID verification audit will be run to detect any mismatches or other problems.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that the second CID card was enabled. Because the data may not match, the CID verification audit will be run.

Recommended Action: If an EM-1020 follows, execute the **CIDrecov** command to get details of the problems found and how to recover. If not, no action is required.

EM-1022

Message: `A CID card access problem has been encountered, please run the CIDrecov tool to get more information and recovery options.`

Message Type: LOG

Severity: WARNING

Probable Cause: Indicates that a problem was encountered while accessing one (or both) of the 2 CID cards or with the content of the data stored there.

Recommended Action:

Execute the **CIDrecov** command to get details of the problems found and how to recover.

EM-1023

Message: `Chassis fan airflow-direction <fan-direction> change is failed.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates failure to change the fan airflow direction.

Recommended Action: No action is required.

EM-1024

Message: `Platform is not supported for changing the fan-airflow direction.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that the platform is not supported for changing the configuration.

Recommended Action: No action is required..

EM-1028

Message: `HIL Error: <function> failed to access history log for FRU: <FRU Id> (rc=<return code>).`

Message Type: FFDC | LOG

Severity: WARNING

Probable Cause: Indicates a problem accessing the data on the Chassis ID (CID) card field-replaceable unit (FRU) or the World Wide Name (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. This error can indicate a significant hardware problem.

The *FRU ID* value is composed of a FRU type string and an optional number to identify the unit, slot, or port. The return code is for internal use only.

Recommended Action: If the problem persists, reload or power cycle the switch.

If the problem still persists, perform one of the following actions:

- For compact switches, replace the switch.

- For CID cards, run the CIDrecov tool to get more information.

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

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 error persists, check for loose or dirty connections. Remove all dust and debris prior to reseating the field-replaceable unit (FRU). Replace the FRU if it continues to fail.

EM-1031

Message: `<FRU Id> ejector not closed.`

Message Type: LOG

Severity: ERROR

Probable Cause: Indicates that the environmental monitor (EM) has found a switch interface module that is inserted, but the optical ejector switch is not latched. The interface module in the specified slot is treated as not inserted.

Recommended Action: Close the ejector switch (completely screw in the optical (middle) thumbscrew on the switch fabric module(SFM)) if the field-replaceable unit (FRU) is intended for use. Refer to the appropriate *Hardware Reference Manual* for instructions on inserting the switch interface modules.

EM-1032

Message: `<FRU Id> is faulted due to a PCI scan failure.`

Message Type: LOG

Severity: ERROR

Probable Cause: Indicates that the interface module in the specified slot has been marked as faulty because the peripheral component interconnect (PCI) scan during interface module validation failed.

Recommended Action: Power cycle or reseat the interface module.

Execute the **diag systemverification** command to verify that the switch does not have hardware problems.

If the problem persists, replace the interface module.

EM-1033

Message: `MM in <FRU Id> is reloading.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that the standby management module has been detected to be in the reload process. The high availability (HA) feature will not be available. This message occurs every time the other management module reloads, even as part of a clean warm . In most situations, this message is followed by the EM-1047 message, and no action is required for the management module; however, if the was not intentional, it is recommended to find the reason for the .

Recommended Action: If the standby management module was just reloaded, wait for the error to clear (execute the **show slots** command to determine if the errors are cleared). Watch for the EM-1047 message to verify that this error has cleared.

If the standby management module state changes to faulty or if it was not intentionally reloaded, check the error logs on the other management module (using the **show logging raslog** 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> is set to faulty, rc=<return code>.`

Message Type: LOG

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 **diag systemverification** command to verify that the switch does not have hardware problems.

If the problem persists, replace the FRU.

EM-1036

Message: `<FRU Id> is not accessible.`

Message Type: LOG

Severity: WARNING

Probable Cause: Indicates that the specified field-replaceable unit (FRU) is not present on the switch.

If the FRU is a Chassis ID (CID) card, then the default WWN and IP addresses are used for the switch.

Recommended Action: Reseat the FRU card.

If the problem persists, reload or power cycle the switch.

Execute the **`diag systemverification`** command to verify that the switch does not have hardware problems.

If the problem still persists, replace the FRU.

EM-1037

Message: `<FRU Id> is no longer faulted.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that the specified power supply is no longer marked faulty; probably because its AC power supply has been turned on.

Recommended Action: No action is required.

EM-1038

Message: `Chassis fan airflow-direction changed to <fan-direction>`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates change of fan airflow direction.

Recommended Action: No action is required.

EM-1039

Message: `Chassis fan airflow-direction changed to <fan-direction>`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates an automatic change of fan airflow direction.

Recommended Action: No action is required.

EM-1042

Message: `Important FRU header data for <FRU Id> is invalid.`

Message Type: LOG

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 it is corrupted in the object database, which contains information about all the FRUs.

Recommended Action: Reseat the FRU. If the problem persists, replace the FRU.

EM-1043

Message: `Cannot power <FRU Id> <state (on or off)>.`

Message Type: LOG

Severity: WARNING

Probable Cause: Indicates that the specified field-replaceable unit (FRU) could not be powered on or off. The FRU is not responding to commands.

Recommended Action: Reseat or replace the FRU.

EM-1045

Message: `<FRU Id> is being powered <new state>.`

Message Type: LOG

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 interface module.

The new state can be one of the following:

- On - A port interface module is being powered on because more power is available (either a power supply was inserted or a port interface module was removed or powered down).
- Off - A port interface module has been powered down because of a (predicted) failure of the power supply.
- Down - A newly inserted port interface module was not powered on because there was not enough power available.

Recommended Action: Refer to the *Hardware Reference Manual* of your switch for the number of power supplies required for redundancy.

EM-1046

Message: `Error status received for interface module ID <id value> for <FRU Id>, <interface module incompatibility type: platform>.`

Message Type: LOG

Severity: WARNING

Probable Cause: Indicates that the specified interface module is incompatible.

Recommended Action: If the interface module ID listed is incorrect, the field-replaceable unit (FRU) header for the interface module is corrupted and the interface module must be replaced.

If the error is due to platform, the interface module ID listed is not supported for that platform (management module) type. Remove the interface module from the chassis.

EM-1047

Message: `MM in <FRU Id> is booting up.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that the firmware in the specified management module is now in the boot process. This message usually follows the EM-1033 message. The new standby management module is in the process of reloading and has turned off the MM_ERR signal.

Recommended Action: No action is required.

EM-1048

Message: `<FRU Id> I2C access recovered: state <current state>.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that the inter-integrated circuit (I2C) bus problems have been resolved and the specified field-replaceable unit (FRU) is accessible on the I2C bus.

Recommended Action: No action is required. This message is displayed when the EM-1029 error is resolved.

EM-1049

Message: `FRU <FRU Id> insertion detected.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that the field-replaceable unit (FRU) of the specified type and location was inserted into the chassis.

Recommended Action: No action is required.

EM-1050

Message: `FRU <FRU Id> removal detected.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that the field-replaceable unit (FRU) of the specified type and location was removed from the chassis.

Recommended Action: Verify that the FRU was intended to be removed. Replace the FRU as soon as possible.

EM-1051

Message: `<FRU Id>: Inconsistency detected, FRU re-initialized.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that an inconsistent state was found in the specified field-replaceable unit (FRU). This event occurs when the state of the FRU was changing during a . The FRU is reinitialized and traffic may have been disrupted.

Recommended Action: No action is required.

EM-1059

Message: `<FRU Id or Switch name> with ID <Interface module Id> may not be supported on this platform, check firmware version as a possible cause.`

Message Type: LOG

Severity: ERROR

Probable Cause: Indicates that the interface module inserted in the specified slot or the switch (for compact switches) is not compatible with the switch configuration software. The interface module will not be completely usable.

The interface module may only be supported by a later (or earlier) version of the firmware.

Recommended Action: Change the management module firmware or replace the interface module. Make sure the replacement is compatible with your switch type and firmware.

EM-1064

Message: `<FRU Id> is being powered off (based on user configuration) upon receiving a HW ASIC ERROR, reason:<Fault reason>.`

Message Type: LOG

Severity: CRITICAL

Probable Cause: Indicates that the interface module has been powered off because a hardware application-specific integrated circuit (ASIC) error was detected, and you have selected to power off the problem interface module when such a condition occurred.

Recommended Action: Execute the **`copy support`** command and contact your switch service provider.

EM-1068

Message: `High Availability Service Management subsystem failed to respond. A required component is not operating.`

Message Type: FFDC | LOG

Severity: ERROR

Probable Cause: Indicates that the high availability (HA) subsystem has not returned a response within 4 minutes of receiving a request from the environmental monitor (EM). This event 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 Network OS configuration or hardware problems on the switch.

Recommended Action: Reload or power cycle the switch.

If the message persists, execute the **`copy support`** command and contact your switch service provider/

EM-1069

Message: `<FRU slot identifier> is being powered off.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that the specified interface module has been intentionally powered off.

Recommended Action: No action is required.

EM-1070

Message: `<FRU slot identifier> is being powered on.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that the specified interface module has been intentionally powered on.

Recommended Action: No action is required.

EM-1080

Message: `<FRU Id> is being faulted (<return code>) because it was so faulted before .`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that the specified interface module or fan was faulted prior to the most recent , and that state and reason code are being carried forward.

Recommended Action: Reseat the FRU.

Execute the **`diag systemverification`** command to verify that the switch does not have hardware problems.

If the problem persists, replace the FRU.

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: CFFDC | LOG

Severity: CRITICAL

Probable Cause: Indicates that 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 in 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

Severity: CRITICAL

Probable Cause: Indicates that 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-1102

Message: `<Fru slot identifier> offline diagnostic mode is turned on.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that the specified interface module is in offline diagnostic mode.

Recommended Action: No action is required.

EM-1103

Message: `<Fru slot identifier> offline diagnostic mode is turned off.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that the specified interface module is not in offline diagnostic mode.

Recommended Action: No action is required.

EM-1104

Message: `<FRU Id> sysFPGA is out of date(<sysFPGA running version>,<sysFPGA latest version>).`

Message Type: LOG

Severity: WARNING

Probable Cause: Indicates that the specified FRU's sysFPGA image is out of date.

Recommended Action: No action is required.

EM-2003

Message: `<FRU Id or switch for compact switches> has failed the POST tests. FRU is being faulted.`

Message Type: LOG

Severity: ERROR

Probable Cause: Indicates that the specified 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. To view this log file you must be logged in at the root level. The login ID is switch name for compact systems.

Recommended Action: On modular systems, reseat the specified FRU.

On compact switches, reload or power cycle the switch.

If the problem persists:

- Execute the **`diag systemverification`** command to verify that the switch does not have hardware problems.
- On modular systems, replace the specified FRU; For compact switch, replace the switch.

ERCP Messages

ERCP-1000

Message: Multiple ECC errors are detected and the system will reload automatically.

Message Type: FFDC | LOG

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.

FABS Messages

FABS-1001

Message: `<Function name> <Description of memory need>.`

Message Type: FFDC | LOG

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 Network OS problem or file corruption. The *Description of memory need* variable specifies the memory size that was being requested. The value could be any whole number.

Recommended Action: Reload or power cycle the switch.

FABS-1002

Message:`<Function name> <Description of problem>.`

Message Type: LOG

Severity: WARNING

Probable Cause: Indicates that an internal problem has been detected by the software. This is usually an internal Network OS problem or file corruption.

Recommended Action: Reload or power cycle the switch.

If the message persists, execute the **`firmware download`** 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

Severity: WARNING

Probable Cause: Indicates that an operation has been interrupted by a signal. This is usually an internal Network OS problem or file corruption.

Recommended Action: Reload or power cycle the switch.

FABS-1005

Message: `<Function name and description of problem> (<ID type>= <ID number>).`

Message Type: LOG

Severity: WARNING

Probable Cause: Indicates that an unsupported operation has been requested. This is usually an internal Network OS problem or file corruption. The following is the possible value for the *Function name and description of problem* variable:

`fabsys_write: Unsupported write operation: process xxx`

The xxx value is the process ID (PID), which could be any whole number.

Recommended Action: Reload or power cycle the active management module (for modular systems) or the switch (for compact systems).

If the message persists, execute the **`firmware download`** command to update the firmware.

FABS-1006

Message: `<Function name and description of problem> object <object type id> unit <slot>.`

Message Type: LOG

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 Network OS data problem on the switch. The following are the possible values for the *function name and description of problem* variable:

- 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_hndlr: 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, fail over or reload the switch.

If the message persists, execute the **`firmware download`** command to update the firmware.

FABS-1007

Message: `<Function name>: Media state is invalid - status=<Status value>.`

Message Type: LOG

Severity: WARNING

Probable Cause: Indicates that the Network OS has detected an invalid value in an object status field. This is usually an internal Network OS problem or file corruption.

Recommended Action: Reload or power cycle the switch.

If the message persists, execute the **`firmware download`** command to update the firmware.

FABS-1008

Message: `<Function name>: Media OID mapping failed.`

Message Type: LOG

Severity: WARNING

Probable Cause: Indicates that the Network OS was unable to locate a necessary object handle. This is usually an internal Network OS problem or file corruption.

Recommended Action: Reload or power cycle the switch.

FABS-1009

Message: `<Function name>: type is not media.`

Message Type: LOG

Severity: WARNING

Probable Cause: Indicates that the Network OS was unable to locate an appropriate object handle. This is usually an internal Network OS problem or file corruption.

Recommended Action: Reload or power cycle the switch.

FABS-1010

Message: `<Function name>: Wrong media_event <Event number>.`

Message Type: LOG

Severity: WARNING

Probable Cause: Indicates that the Network OS detected an unknown event type. This is usually an internal Network OS problem or file corruption

Recommended Action: Reload or power cycle the switch.

If the message persists, execute the **`firmware download`** command to update the firmware.

FABS-1011

Message: `<Method name>[<Method tag number>]:Invalid input state 0x<Input state code>.`

Message Type: LOG

Severity: ERROR

Probable Cause: Indicates that an unrecognized state code was used in an internal Network OS message for a field-replaceable unit (FRU).

Recommended Action: Reload or power cycle the management module or switch.

If the message persists, execute the <cmd>firmware download</cmd> command to update the firmware.

FABS-1013

Message: `<Method name>[<Method tag number>]:Unknown interface module type 0x<Interface module type>.`

Message Type: LOG

Severity: ERROR

Probable Cause: Indicates that an unrecognized type of interface module has been discovered in the system.

Recommended Action: This error can be caused by one of the following reasons: an incorrect field-replaceable unit (FRU) header, inability to read the FRU header, or the interface module may not be supported by this platform or Network OS version.

Verify that the interface module is valid for use in this system and this version of Network OS.

Reseat the interface module.

If this is a valid interface module and reseating does not solve the problem, replace the interface module.

FABS-1014

Message: `<Method name>[<Method tag number>]:Unknown FRU type 0x<FRU Object type>.`

Message Type: LOG

Severity: ERROR

Probable Cause: Indicates that an unrecognized type of field-replaceable unit (FRU) has been discovered in the system.

Recommended Action: This error can be caused by one of the following reasons: an incorrect FRU header, inability to read the FRU header, or the FRU may not be supported by this platform or Network OS version.

Verify that the FRU is valid for use in this system and this version of Network 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>[<Method tag number>]:Request to enable FRU type 0x<Arg>FRU Object type>, unit <Unit number> failed. err code <Error code>.`

Message Type: LOG

Severity: ERROR

Probable Cause: Indicates that the specified field-replaceable unit (FRU) could not be enabled. This is usually an internal Network OS problem.

Recommended Action: Remove and reinsert the FRU.

Reload or power cycle the management module or switch.

If the message persists, execute the **`firmware download`** command to update the firmware.

FSS Messages

FSS-1001

Message: `Component (<component name>) dropping HA data update (<update ID>).`

Message Type: LOG

Severity: WARNING

Probable Cause: Indicates that an application has dropped a high availability (HA) data update.

Recommended Action: Execute the copy support 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

Severity: WARNING

Probable Cause: Indicates that an application has sent too many concurrent high availability (HA) data updates.

Recommended Action: Execute the copy support 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

Severity: WARNING

Probable Cause: Indicates that the fabric synchronization service (FSS) has dropped the update because an application has not set the transaction flag correctly.

Recommended Action: Execute the copy support command and contact your switch service provider.

FSS-1004

Message: `FSS out of memory (<memory allocation with number of bytes>).`

Message Type: LOG

Severity: ERROR

Probable Cause: Indicates that the system ran out of memory.

Recommended Action: Check memory usage on the switch using the show process memory command.

Execute the copy support command and contact your switch service provider.

FSS-1005

Message: `FSS read failure.`

Message Type: LOG

Severity: WARNING

Probable Cause: Indicates that the read system call to the fabric synchronization service (FSS) device has failed.

Recommended Action: If the message persists, execute the copy support command and contact your switch service provider.

FSS-1006

Message: `No FSS message available.`

Message Type: LOG

Severity: WARNING

Probable Cause: Probable Cause Indicates that data is not available on the fabric synchronization service (FSS) device.

Recommended Action: If the message persists, execute the copy support command and contact your switch service provider.

FSS-1007

Message: `<component name>: Faulty Ethernet connection.`

Message Type: LOG | FFDC

Severity: CRITICAL

Probable Cause: Indicates that the Ethernet connection between the active and standby management modules is not healthy. The error occurs when the standby management module does not respond to a request from the active management module within 5 seconds. This usually indicates a problem with the internal Ethernet connection and a disruption of the synchronization process.

Recommended Action: Execute the copy support command and contact your switch service provider.

FSS-1008

Message: `FSS Error on service component [<service name><service instance>:<component name>]: <Error Message>.`

Message Type: LOG

Severity: CRITICAL

Probable Cause: Indicates that a fabric synchronization service (FSS) error has occurred.

Recommended Action: Execute the copy support command and contact your switch service provider.

FSS-1009

Message: `FSS Error on service instance [<service name><service instance>]: <Error Message>.`

Message Type: LOG

Severity: ERROR

Probable Cause: Indicates that a fabric synchronization service (FSS) error has occurred.

Recommended Action: Execute the copy support command and contact your switch service provider.

FSS-1010

Message: `FSS Warning: <%s>.`

Message Type: LOG

Severity: WARNING

Probable Cause: Indicates that a fabric synchronization service (FSS) error may have occurred.

Recommended Action: No action is required.

FSS-1011

Message: `All services complete the critical recoveries in <time taken for the critical service recovery> sec.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates a non-disruptive with warm recovery.

Recommended Action: If the time taken for critical service recovery is more than 8 seconds, contact your switch service provider.

FSS-1012

Message: `FSS transport flow hitting the threhold (<number of waiting requests>:<the current xmb allocation size>:<total of KERNEL memory>:<total of ATOMIC memory>).`

Message Type: LOG | FFDC

Severity: CRITICAL

Probable Cause: Indicates that the underlying transport is not healthy.

Recommended Action: Execute the copy support command and contact your switch service provider.

FSS-1013

Message: `FSS transport flow hitting OOM (<the current xmb allocation size>).`

Message Type: LOG | FFDC

Severity: CRITICAL

Probable Cause: Indicates out of memory.

Recommended Action: Execute the copy support command and contact your switch service provider.

FSS-1014

Message: `FSS transport is being blocked for too long (<the current xmb allocation size>).`

Message Type: LOG | FFDC

Severity: CRITICAL

Probable Cause: Indicates that fabric synchronization service (FSS) transport has been blocked for too long time.

Recommended Action: Execute the copy support command and contact your switch service provider.

FW Messages

FW-1001

Message:`<label>, value has changed(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that the internal temperature of the switch has changed.

Recommended Action: Respond to this message as is appropriate to the particular policy of the end-user installation. To prevent recurring messages, disable the changed alarm for this threshold. 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.

FW-1002

Message: `<Label>, is below low boundary (High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type: LOG

Severity: WARNING

Probable Cause: Indicates that the internal temperature of the switch has fallen below the low boundary.

Recommended Action: Respond to this message as is appropriate to the particular policy of the end-user installation. Typically, low temperatures means that the fans and airflow of a switch are functioning normally.

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.

FW-1003

Message: `<Label>, is above high boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type: LOG

Severity: WARNING

Probable Cause: Indicates that the internal temperature of the switch has risen above the high boundary to a value that may damage the switch.

Recommended Action: This message generally appears when a fan fails. If so, a fan-failure message accompanies this message. Replace the fan.

FW-1004

Message: `<Label>, is between high and low boundaries(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that the internal temperature of the switch has changed from a value outside of the acceptable range to a value within the acceptable range.

Recommended Action: Respond to this message as is appropriate to the particular policy of the end-user installation. 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.

FW-1005

Message: `<Label>, value has changed(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that the speed of the fan has changed. Fan problems typically contribute to temperature problems.

Recommended Action: No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation. Consistently abnormal fan speeds generally indicate that the fan is malfunctioning.

FW-1006

Message: `<Label>, value has changed(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type: LOG

Severity: WARNING

Probable Cause: Indicates that the speed of the fan has changed. Fan problems typically contribute to temperature problems.

Recommended Action: No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation. Consistently abnormal fan speeds generally indicate that the fan is malfunctioning.

FW-1007

Message: `<Label>, is above high boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type: LOG

Severity: WARNING

Probable Cause: Indicates that the speed of the fan has risen above the high boundary. Fan problems typically contribute to temperature problems.

Recommended Action: Consistently abnormal fan speeds generally indicate that the fan is failing. Replace the fan.

FW-1008

Message: `<Label>, is between high and low boundaries(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that the speed of the fan has changed from a value outside of the acceptable range to a value within the acceptable range. Fan problems typically contribute to temperature problems.

Recommended Action: No action is required. Consistently abnormal fan speeds generally indicate that the fan is failing. If this message occurs repeatedly, replace the fan.

FW-1009

Message: `<Label>, value has changed (High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that the state of the power supply has changed from faulty to functional or from functional to faulty.

Recommended Action: If the power supply is functioning correctly, no action is required.

If the power supply is functioning below the acceptable boundary, verify that it is seated correctly in the chassis. Execute the **`show environment power`** command to view the status of the power supply. If the power supply continues to be a problem, replace the faulty power supply.

FW-1010

Message: `<Label>, is below low boundary (High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type: LOG

Severity: WARNING

Probable Cause: Indicates that the power supply is faulty. The power supply is not producing enough power.

Recommended Action: Verify that the power supply is installed correctly and that it is correctly seated in the chassis. If the problem persists, replace the faulty power supply.

FW-1012

Message: `<Label>, is between high and low boundaries(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that the power supply counter changed from a value outside of the acceptable range to a value within the acceptable range.

Recommended Action: No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

FW-1034

Message: `<Label>, is below low boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type: LOG

Severity: WARNING

Probable Cause: Indicates that the temperature of the small form-factor pluggable (SFP) transceiver has fallen below the low boundary.

Recommended Action: No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

FW-1035

Message: `<Label>, is above high boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type: LOG

Severity: WARNING

Probable Cause: Indicates that the temperature of the small form-factor pluggable (SFP) transceiver has risen above the high boundary.

Recommended Action: Frequent fluctuations in temperature may indicate a deteriorating SFP transceiver. Replace the SFP transceiver.

FW-1036

Message: `<Label>, is between high and low boundaries(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that the temperature of the small form-factor pluggable (SFP) transceiver has changed from a value outside of the acceptable range to a value within the acceptable range.

Recommended Action: No action is required.

FW-1038

Message: `<Label>, is below low boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type: LOG

Severity: WARNING

Probable Cause: Indicates that the receive power value of the small form-factor pluggable (SFP) transceiver has fallen below the low boundary. The receive performance area measures the amount of incoming laser to help you determine if the SFP transceiver is in good working condition or not. If the counter often exceeds the threshold, the SFP transceiver is deteriorating.

Recommended Action: Verify that the optical components are clean and functioning properly. Replace deteriorating cables or SFP transceivers. Check for damage from heat or age.

FW-1039

Message: `<Label>, is above high boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type: LOG

Severity: WARNING

Probable Cause: Indicates that the receive power value of the small form-factor pluggable (SFP) transceiver has risen above the high boundary. The receive performance area measures the amount of incoming laser to help you determine if the SFP transceiver is in good working condition or not. If the counter often exceeds the threshold, the SFP transceiver is deteriorating.

Recommended Action: Replace the SFP transceiver before it deteriorates.

FW-1040

Message: `<Label>, is between high and low boundaries(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that the receive power value of the small form-factor pluggable (SFP) transceiver has changed from a value outside of the acceptable range to a value within the acceptable range. The receive performance area measures the amount of incoming laser to help you determine if the SFP transceiver is in good working condition or not. If the counter often exceeds the threshold, the SFP transceiver is deteriorating.

Recommended Action: No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

FW-1042

Message: `<Label>, is below low boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type: LOG

Severity: WARNING

Probable Cause: Indicates that the transmit power value of the small form-factor pluggable (SFP) transceiver has fallen below the low boundary. The transmit performance area measures the amount of outgoing laser to help you determine if the SFP transceiver is in good working condition or not. If the counter often exceeds the threshold, the SFP transceiver is deteriorating.

Recommended Action: Verify that the optical components are clean and functioning properly. Replace deteriorating cables or SFP transceivers. Check for damage from heat or age.

FW-1043

Message: `<Label>, is above high boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type: LOG

Severity: WARNING

Probable Cause: Indicates that the transmit power value of the small form-factor pluggable (SFP) transceiver has risen above the high boundary. The transmit performance area measures the amount of outgoing laser to help you determine if the SFP transceiver is in good working condition or not. If the counter often exceeds the threshold, the SFP transceiver is deteriorating.

Recommended Action: Replace the SFP transceiver.

FW-1044

Message: `<Label>, is between high and low boundaries(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that the transmit power value of the small form-factor pluggable (SFP) transceiver has changed from a value outside of the acceptable range to a value within the acceptable range. The transmit performance area measures the amount of outgoing laser to help you determine if the SFP transceiver is in good working condition or not. If the counter often exceeds the threshold, the SFP transceiver is deteriorating.

Recommended Action: No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

FW-1046

Message: `<Label>, is below low boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type: LOG

Severity: WARNING

Probable Cause: Indicates that the value of the small form-factor pluggable (SFP) transceiver voltage has fallen below the low boundary.

Recommended Action: Verify that the optical components are clean and functioning properly. Replace deteriorating cables or SFP transceivers. Check for damage from heat or age.

FW-1047

Message: `<Label>, is above high boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type: LOG

Severity: WARNING

Probable Cause: Indicates that the value of the small form-factor pluggable (SFP) transceiver voltage has risen above the high boundary.

Recommended Action: The supplied current of the SFP transceiver is outside of the normal range, indicating possible hardware failure. If the current rises above the high boundary, replace the SFP transceiver.

FW-1048

Message: `<Label>, is between high and low boundaries(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that the value of the small form-factor pluggable (SFP) transceiver voltage has changed from a value outside of the acceptable range to a value within the acceptable range.

Recommended Action: No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

FW-1050

Message: `<Label>, is below low boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type: LOG

Severity: WARNING

Probable Cause: Indicates that the value of the small form-factor pluggable (SFP) transceiver has fallen below the low boundary.

Recommended Action: Configure the low threshold to 1 so that the threshold triggers an alarm when the value falls to 0 (Out_of_Range). If continuous or repeated alarms occur, replace the SFP transceiver before it deteriorates.

FW-1051

Message: `<Label>, is above high boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type: LOG

Severity: WARNING

Probable Cause: Indicates that the value of the small form-factor pluggable (SFP) transceiver voltage has risen above the high boundary. High voltages indicate possible hardware failures.

Recommended Action: Frequent voltage fluctuations are an indication that the SFP transceiver is deteriorating. Replace the SFP transceiver.

FW-1052

Message: `<Label>, is between high and low boundaries(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that the value of the small form-factor pluggable (SFP) transceiver voltage has changed from a value outside of the acceptable range to a value within the acceptable range.

Recommended Action: No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

FW-3101

Message: `<Label>, is below low boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that the number of invalid cyclic redundancy checks (CRCs) that the port experiences has fallen below the low boundary.

Recommended Action: No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation. A low number of invalid CRCs means the switch is functioning normally.

FW-3102

Message: `<Label>, is above high boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type: LOG

Severity: WARNING

Probable Cause: Indicates that the number of invalid cyclic redundancy checks (CRCs) that the port experiences has risen above the high boundary.

Recommended Action: This error generally indicates an deteriorating fabric hardware. Check small form-factor pluggable (SFP) transceivers, cables, and connections for faulty hardware. Verify that all optical hardware is clean.

FW-3103

Message: `<Label>, is between high and low boundaries(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that the number of invalid cyclic redundancy checks (CRCs) that the port experiences has changed from a value outside of the acceptable range to a value within the acceptable range.

Recommended Action: Respond to this message as is appropriate to the particular policy of the end-user installation. Frequent fluctuations in CRC errors generally indicate an aging fabric. Check the small form-factor pluggable (SFP) transceivers, cables, and connections for faulty hardware. Verify that all optical hardware is clean.

FW-3104

Message: `<Label>, has crossed lower threshold boundary to in between(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that the number of invalid cyclic redundancy checks (CRCs) that the port experiences crossed lower threshold boundary to a value within the acceptable range.

Recommended Action: Respond to this message as is appropriate to the particular policy of the end-user installation. Frequent fluctuations in CRC errors generally indicate an aging fabric. Check small form-factor pluggable (SFP) transceivers, cables, and connections for faulty hardware. Verify that all optical hardware is clean.

FW-3105

Message: `<Label>, has dropped below upper threshold boundary to in between(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that the number of invalid cyclic redundancy checks (CRCs) that the port experiences has dropped below upper threshold boundary to a value within the acceptable range.

Recommended Action: Respond to this message as is appropriate to the particular policy of the end-user installation. Frequent fluctuations in CRC errors generally indicate an aging fabric. Check small form-factor pluggable (SFP) transceivers, cables, and connections for faulty hardware. Verify that all optical hardware is clean.

FW-3107

Message: `<Label>, is below low boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that the number of Abnormal Frame termination frames that the port experiences has fallen below the low boundary.

Recommended Action: No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation. A low number of abnormal frame termination errors means the system is operating normally.

FW-3108

Message: `<Label>, is above high boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type: LOG

Severity: WARNING

Probable Cause: Indicates that the number of abnormal frame termination frames that the port experiences has risen above the high boundary. Flapping interfaces during the traffic flow can generate this error.

Recommended Action: Check all loose connections in the fabric.

FW-3109

Message: `<Label>, is between high and low boundaries(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that the number of abnormal frame termination frames that the port experiences has changed from a value outside of the acceptable range to a value within the acceptable range.

Recommended Action: Respond to this message as is appropriate to the particular policy of the end-user installation. Check all loose connections in the fabric.

FW-3110

Message: `<Label>, has crossed lower threshold boundary to in between(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that the number of abnormal frame termination frames that the port experiences crossed lower threshold boundary to a value within the acceptable range.

Recommended Action: Respond to this message as is appropriate to the particular policy of the end-user installation. Check all loose connections in the fabric.

FW-3111

Message: `<Label>, has dropped below upper threshold boundary to in between(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that the number of abnormal frame termination frames that the port experiences has dropped below upper threshold boundary to a value within the acceptable range.

Recommended Action: Respond to this message as is appropriate to the particular policy of the end-user installation. Check all loose connections in the fabric.

FW-3113

Message: `<Label>, is below low boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that the number of frames with symbol error that the port experiences has fallen below the low boundary.

Recommended Action: Respond to this message as is appropriate to the particular policy of the end-user installation. A low number of symbol errors means the system is operating normally.

FW-3114

Message: `<Label>, is above high boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type: LOG

Severity: WARNING

Probable Cause: Indicates that the number of frames with symbol error that the port experiences has risen above the high boundary. Flapping interfaces or loose connections can cause this error.

A high number of symbol errors indicate a deteriorated device, cable, or hardware.

Recommended Action: Check your small form-factor pluggables (SFPs), cables, and connections for faulty hardware. Verify that all optical hardware is clean.

FW-3115

Message: `<Label>, is between high and low boundaries(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that the number of frames with symbol error that the port experiences has changed from a value outside of the acceptable range to a value within the acceptable range.

Recommended Action: Respond to this message as is appropriate to the particular policy of the end-user installation. Check all cables and form factors in the system.

FW-3116

Message: `<Label>, has crossed lower threshold boundary to in between(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that the number of frames with symbol error that the port experiences crossed lower threshold boundary to a value within the acceptable range.

Recommended Action: Respond to this message as is appropriate to the particular policy of the end-user installation. Check all cables and form factors in the system.

FW-3117

Message: `<Label>, has dropped below upper threshold boundary to in between(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that the number of frames with symbol error that the port experiences has dropped below upper threshold boundary to a value within the acceptable range.

Recommended Action: Respond to this message as is appropriate to the particular policy of the end-user installation. Check all cables and form factors in the system.

FW-3119

Message: `<Label>, is below low boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that the number of inter frame gap violation errors that the port experiences has fallen below the low boundary.

Recommended Action: Respond to this message as is appropriate to the particular policy of the end-user installation. A low number of inter frame gap errors means the system is operating normally.

FW-3120

Message: `<Label>, is above high boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type: LOG

Severity: WARNING

Probable Cause: Indicates that the number of inter frame gap violation errors that the port experiences has risen above the high boundary. Flapping interfaces during the traffic flow can generate this error. Congestion or transmitting multiple frames without an inter frame gap.

Recommended Action: Check loose connections and congestion in the fabric.

FW-3121

Message: `<Label>, is between high and low boundaries(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that the number of inter frame gap violation errors that the port experiences has changed from a value outside of the acceptable range to a value within the acceptable range.

Recommended Action: Respond to this message as is appropriate to the particular policy of the end-user installation. Check loose connections and congestion in the fabric.

FW-3122

Message: `<Label>, has crossed lower threshold boundary to in between(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that the number of inter frame gap violation errors that the port experiences crossed lower threshold boundary to a value within the acceptable range.

Recommended Action: Respond to this message as is appropriate to the particular policy of the end-user installation. Check loose connections and congestion in the fabric.

FW-3123

Message: `<Label>, has dropped below upper threshold boundary to in between(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that the number of inter frame gap violation errors that the port experiences has dropped below upper threshold boundary to a value within the acceptable range.

Recommended Action: Respond to this message as is appropriate to the particular policy of the end-user installation. Check loose connections and congestion in the fabric.

FW-1297

Message: `<Label>, is below low boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that the number of Telnet violations has fallen below the low boundary. Telnet violations indicate that a Telnet connection request has been received from an unauthorized IP address. The TELNET_POLICY contains a list of IP addresses that are authorized to establish Telnet connections to switches in the fabric.

Recommended Action: No action is required.

FW-1298

Message: `<Label>, is above high boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type: LOG

Severity: WARNING

Probable Cause: Indicates that the number of Telnet violations has risen above the high boundary. Telnet violations indicate that a Telnet connection request has been received from an unauthorized IP address. The TELNET_POLICY contains a list of IP addresses that are authorized to establish Telnet connections to switches in the fabric.

Recommended Action: Execute the **`show logging raslog`** command 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.

FW-1299

Message: `<Label>, is between high and low boundaries(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that the number of Telnet violations has changed from a value outside of the acceptable range to a value within the acceptable range. Telnet violations indicate that a Telnet connection request has been received from an unauthorized IP address. The TELNET_POLICY contains a list of IP addresses that are authorized to establish Telnet connections to switches in the fabric.

Recommended Action: No action is required.

FW-1341

Message: `<Label>, is below low boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that the number of login violations has fallen below the low boundary. Login violations indicate that a login failure has been detected.

Recommended Action: No action is required.

FW-1342

Message: `<Label>, is above high boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type: LOG

Severity: WARNING

Probable Cause: Indicates that the number of login violations has risen above the high boundary. Login violations indicate that a login failure has been detected.

Recommended Action: Execute the **`show logging raslog`** command to determine the IP address of the log in attempt. Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

FW-1343

Message: `<Label>, is between high and low boundaries(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that the number of login violations has changed from a value outside of the acceptable range to a value within the acceptable range. Login violations indicate that a login failure has been detected.

Recommended Action: No action is required.

FW-1403

Message: `<Label>, is between high and low boundaries(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that the CPU or memory usage is between the boundary limits.

Recommended Action: No action is required.

FW-1404

Message: `<Label>, is above high boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type: LOG

Severity: WARNING

Probable Cause: Indicates that the CPU or memory usage is above the configured threshold. If this message pertains to memory usage, then the usage is above middle memory threshold.

Recommended Action: No action is required.

FW-1405

Message: `<Label>, is above high boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that the memory usage is above low threshold.

Recommended Action: No action is required.

FW-1406

Message: `<Label>, is above high boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type: LOG

Severity: CRITICAL

Probable Cause: Indicates that the memory usage is above the configured high threshold for memory usage.

Recommended Action: No action is required.

FW-1407

Message: `<Label>, is between high and low boundaries(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that the memory usage is between the configured high and medium thresholds for memory usage.

Recommended Action: No action is required.

FW-1408

Message: `<Label>, is between high and low boundaries(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that the memory usage is between the configured low and medium thresholds for memory usage.

Recommended Action: No action is required.

FW-1409

Message: `Current disk utilization is <Value> <Unit>. Deleting <File>.`

Message Type: LOG

Severity: WARNING

Probable Cause: Indicates high compact flash (CF) disk utilization.

Recommended Action: No action is required.

FW-1410

Message: `Disk usage is greater than 60 percent and max number of Core file limit [5] has been exceeded. Deleting the oldest core file: <File>.`

Message Type: LOG

Severity: WARNING

Probable Cause: Indicates that the maximum number of core file limit has been exceeded.

Recommended Action: No action is required.

FW-1411

Message: `Early out-of-memory condition detected. System critically low on available memory. <free-memory-value> is below the set threshold <free-memory-threshold-value>. Shutting down all interfaces.`

Message Type: LOG

Severity: CRITICAL

Probable Cause: Out of memory error.

Recommended Action: None. Device is shut down automatically due to out-of-memory condition.

FW-1412

Message: `EarlyOOM debug logs collected. Refer logs at /var/log/threshold/mem/.`

Message Type: LOG

Severity: INFO

Probable Cause: Out of memory.

Recommended Action: Use support save collection for further debugging.

FW-1413

Message: `<device-name>, DISK ALERT: <alert-sequence-number> <monitored-partition> space [ crossed below | further reduced below ] threshold (available <remaining-space-in-mb>)`

Message Type: LOG

Severity: CRITICAL

Probable Cause: Low disk space alert.

Recommended Action: Clean the identified partition by removing unnecessary files.

There is a possibility that this message is generated multiple times. Each message is generated with a sequence number to identify when the message was generated. A maximum of 10 messages are generated. Also, if the available space falls below 100 MB, then this message is not generated.

FW-1414

Message: `<device-name>, DISK ALERT: <number> core file(s) removed from <directory>. Check <log-file-name> for details.`

Message Type: LOG

Severity: INFO

Probable Cause: Stored log files were automatically deleted from the specified location.

Recommended Action: No action is required.

FW-1415

Message: `<device-name> DISK ALERT: <monitored-partition> recovered above threshold. (available <remaining-space-in-mb>)`

Message Type: LOG

Severity: INFO

Probable Cause: The monitored partition has been freed up of space and has returned to above threshold level.

Recommended Action: No action is required.

FW-1424

Message: `Switch status changed from <Previous state> to <Current state>.`

Message Type: LOG

Severity: WARNING

Probable Cause: Indicates that the switch is not in a healthy state. This occurred because of a policy violation.

Recommended Action: Execute the **`show system monitor`** command to determine the policy violation.

FW-1425

Message: `Switch status changed from <Bad state> to HEALTHY.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that the switch status has changed to a healthy state. This state change occurred because a policy is no longer violated.

Recommended Action: No action is required.

FW-1426

Message: `Switch status change contributing factor Power supply: <Number Bad> bad, <Number Missing> absent.`

Message Type: LOG

Severity: WARNING

Probable Cause: Indicates that the switch is not in a healthy state. This occurred because the number of faulty or missing power supplies is greater than or equal to the policy set by the **`system-monitor`** command.

Recommended Action: Replace the faulty or missing power supplies.

FW-1427

Message: `Switch status change contributing factor Power supply: <Number Bad> bad.`

Message Type: LOG

Severity: WARNING

Probable Cause: Indicates that the switch is not in a healthy state. This occurred because the number of faulty power supplies is greater than or equal to the policy set by the **`system-monitor`** command.

Recommended Action: Replace the faulty power supplies.

FW-1428

Message: `Switch status change contributing factor Power supply: <Number Missing> absent.`

Message Type: LOG

Severity: WARNING

Probable Cause: Indicates that the switch is not in a healthy state. This occurred because the number of missing power supplies is greater than or equal to the policy set by the **`system-monitor`** command.

Recommended Action: Replace the missing power supplies.

FW-1429

Message: `Switch status change contributing factor: Power supplies are not redundant.`

Message Type: LOG

Severity: WARNING

Probable Cause: Indicates that the switch is not in a healthy state. This occurred because the power supplies are not in the correct slots for redundancy.

Recommended Action: Rearrange the power supplies so that one is in an odd slot and another in an even slot to make them redundant.

FW-1430

Message: `Switch status change contributing factor <string>.`

Message Type: LOG

Severity: WARNING

Probable Cause: Indicates that the switch is not in a healthy state. This occurred because the number of faulty temperature sensors is greater than or equal to the policy set by the **`system-monitor`** command. A temperature sensor is faulty when the sensor value is not in the acceptable range.

Recommended Action: Replace the field-replaceable unit (FRU) with the faulty temperature sensor.

FW-1431

Message: `Switch status change contributing factor Fan: <Number Bad> bad.`

Message Type: LOG

Severity: WARNING

Probable Cause: Indicates that the switch is not in a healthy state. This occurred because the number of faulty fans is greater than or equal to the policy set by the **`system-monitor`** command. A fan is faulty when sensor value is not in the acceptable range.

Recommended Action: Replace the faulty or deteriorating fans.

FW-1432

Message: `Switch status change contributing factor Cid-Card: <Number Bad> bad.`

Message Type: LOG

Severity: WARNING

Probable Cause: Indicates that the switch is not in a healthy state. This occurred because the number of faulty Chassis ID (CID) cards is greater than or equal to the policy set by the **system-monitor** command.

Recommended Action: Replace the faulty CID card.

FW-1433

Message: `Switch status change contributing factor non-redundant MM : M<CP Number> <MM Status>.`

Message Type: LOG

Severity: WARNING

Probable Cause: Indicates that the switch is not in a healthy state. This occurred because the number of faulty management modules is greater than or equal to the policy set by the **system-monitor** command. The management modules are non-redundant.

Recommended Action: Execute the **show firmware** command to verify if both the management modules have compatible firmware levels. Execute the **firmware download** command to install the same level of firmware to both management modules. Replace any faulty management modules.

If you reset the micro-switch (the latch on the management module) on the active management module before the heartbeat was up on a power cycle, and the management modules came up non-redundant, reload the management modules again to clear the problem.

FW-1434

Message: `Switch status change contributing factor LC: <Number Bad> LC failures (<LC Numbers>).`

Message Type: LOG

Severity: WARNING

Probable Cause: Indicates that the switch is not in a healthy state. This occurred because the number of line card (LC) failures is greater than or equal to the policy set by the **system-monitor** command.

Recommended Action: Replace the faulty LC.

FW-1447

Message: `Switch status change contributing factor SFM: <Number Bad> SFM failures (<Switch State>).`

Message Type: LOG

Severity: WARNING

Probable Cause: Indicates that the switch is not in a healthy state. This occurred because the number of switch fabric module (SFM) failures is greater than or equal to the policy set by the **`system-monitor`** command.

Recommended Action: Replace the faulty SFM.

FW-1435

Message: `Switch status change contributing factor Flash: usage out of range.`

Message Type: LOG

Severity: WARNING

Probable Cause: Indicates that the switch is not in a healthy state. This occurred because the flash usage is out of range. The policy was set using the **`system-monitor`** command.

Recommended Action: Execute the **`clear support`** command to clear the kernel flash.

FW-1439

Message: `Switch status change contributing factor Switch offline.`

Message Type: LOG

Severity: WARNING

Probable Cause: Indicates that the switch is not in a healthy state. This occurred because the switch is offline.

Recommended Action: Execute the **`chassis enable`** command to bring the switch online.

FW-1440

Message: `<FRU label> state has changed to <FRU state>.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that the state of the specified field-replaceable unit (FRU) has changed to "absent".

Recommended Action: Verify if the event was planned. If the event was planned, no action is required. If the event was not planned, check with your system administrator on the hardware state change.

FW-1441

Message: `<FRU label> state has changed to <FRU state>.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that the state of the specified field-replaceable unit (FRU) has changed to "inserted". This means that an FRU is inserted but not powered on.

Recommended Action: Verify if the event was planned. If the event was planned, no action is required. If the event was not planned, check with your system administrator on the hardware state change.

FW-1442

Message: `<FRU label> state has changed to <FRU state>.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that the state of the specified field-replaceable unit (FRU) has changed to "on".

Recommended Action: Verify if the event was planned. If the event was planned, no action is required. If the event was not planned, check with your system administrator on the hardware state change.

FW-1443

Message: `<FRU label> state has changed to <FRU state>.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that the state of the specified field-replaceable unit (FRU) has changed to "off".

Recommended Action: Verify if the event was planned. If the event was planned, no action is required. If the event was not planned, check with your system administrator on the hardware state change.

FW-1444

Message: `<FRU label> state has changed to <FRU state>.`

Message Type: LOG

Severity: WARNING

Probable Cause: Indicates that the state of the specified field-replaceable unit (FRU) has changed to "faulty".

Recommended Action: Replace the FRU.

FW-1500

Message: `Mail overflow - Alerts being discarded.`

Message Type: LOG

Severity: WARNING

Probable Cause: Indicates that a mail alert overflow condition has occurred.

Recommended Action: Resolve or disable the mail alert using the **`system-monitor-mail fru`** command.

FW-1501

Message: `Mail overflow cleared - <Mails discarded> alerts discarded.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that the mail overflow condition has cleared

Recommended Action: No action is required.

FW-1510

Message: `<Area string> threshold exceeded: Port <Port number> disabled.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that the specified port is now disabled because the link on this port had multiple link failures that exceed Fabric Watch (FW) threshold on the port. The link failures occurred due to one of following reasons:

- Physical and hardware problems on the switch.
- Loss of synchronization.

- Hardware failures.
- A defective small form-factor pluggable (SFP) transceiver or faulty cable.

Protocol errors indicates cyclic redundancy check (CRC) sum disparity. Occasionally, these errors occur due to software glitches. Persistent errors occur due to hardware problems.

Recommended Action: Check for concurrent loss of synchronization errors. Check the SFP transceiver and the cable and enable the port using the **`no shutdown`** command.

FW-1511

Message: `CPU 10G <CPU 10G port name> port link down detected.`

Message Type: LOG

Severity: ERROR

Probable Cause: Indicates CPU 10G link is down

Recommended Action: No action is required.

FW-1512

Message: `CPU 10G <CPU 10G port name> port link recovery is started.`

Message Type: LOG

Severity: ERROR

Probable Cause: Indicates CPU 10G link recovery is triggered.

Recommended Action: No action is required.

HASM Messages

HASM-1000

Message: `Daemon <Component name> terminated. System initiated reload/ for recovery.`

Message Type:LOG

Severity:CRITICAL

Probable Cause: Indicates that the software watchdog detected termination of a daemon and the system will reload or to recover.

Recommended Action: After the system reloads, execute the copy support command and contact your switch service provider.

HASM-1002

Message: `Error happens on service instance <Service type name> <Service instance name>: <Error message> (Critical).`

Message Type:LOG | FFDC

Severity:CRITICAL

Probable Cause: Indicates software failure.

Recommended Action: Execute the copy support command and reload the system manually to recover.

HASM-1003

Message: `Error happened on service instance <Service type name> <Service instance name>: <Error message>.`

Message Type:LOG

Severity:WARNING

Probable Cause: Indicates a software error such as mismatch in the fabric synchronization service (FSS) configuration.

Recommended Action: Execute the copy support command and reload the system manually to recover.

HASM-1004

Message: `<Blade name> Processor reloaded - <Reboot Reason>.`

Message Type: AUDIT | LOG

Class: SECURITY

Severity: INFO

Probable Cause: Indicates that the system has been reloaded either because of a user action or an error. The switch reload can be initiated by one of the following commands: firmware download, fastboot, and reload. Some examples of errors that may initiate this message are hardware errors, software errors, compact flash (CF) errors, or memory errors. The reason for reload can be any of the following:

•

• 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
- Reload:API
- Reload:HAM
- EMFault:EM

Recommended Action: Check the error log on both management modules for additional messages that may indicate the reason for the switch reload.

HASM-1013

Message: `Restartable daemon (<Component name>) terminated prematurely. System initiated /reload for recovery.`

Message Type: LOG

Severity: CRITICAL

Probable Cause: Indicates that a restartable daemon terminated before the system has booted up completely.

Recommended Action: After the system reloads, execute the **`copy support`** command and contact your switch service provider.

HASM-1014

Message: `Daemon (<Component name>) terminated while the system was booting up.`

Message Type: LOG

Severity: CRITICAL

Probable Cause: Indicates that a daemon terminated before the system has booted up completely.

Recommended Action: Execute the **`copy support`** command and reload the system manually to recover.

HASM-1015

Message: `Error happens on service instance <Service type name> <Service instance name>: <Error message> (Critical, reboot to recover).`

Message Type: LOG | FFDC

Severity: CRITICAL

Probable Cause: Indicates software failure.

Recommended Action: Execute the **`copy support`** command after the system boots up.

HASM-1016

Message: `Daemon (<Component name>) was successfully restarted after termination.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that a daemon was successfully restarted after being terminated.

Recommended Action: No action is required.

HASM-1020

Message: `Firmware operation (<operation code>) was aborted due to timeout.`

Message Type: LOG | FFDC |

Severity: WARNING

Probable Cause: Indicates that the firmware operation took too long to complete due to CPU overload or other software errors.

Recommended Action: No action is required. Firmware commit will be started automatically to repair the compact flash (CF) partitions in the system.

HASM-1021

Message: `Firmware operation (<operation code>) was aborted manually.`

Message Type: LOG |

Severity: WARNING

Probable Cause: Indicates that the specified firmware operation was aborted manually.

Recommended Action: No action is required.

HASM-1022

Message: `Failed to fork firmware child process.`

Message Type: LOG |

Severity: WARNING

Probable Cause: Indicates that the firmware operation could not be started due to a software error.

Recommended Action: Execute the **`copy support`** command and contact your switch service provider.

HASM-1026

Message: `The last reboot is due to Kernel Panic in <Module name>.`

Message Type: LOG

Severity: WARNING

Probable Cause: Indicates that the system has reloaded due to kernel panic in the specified module.

Recommended Action: Execute the **`copy support`** command and contact your switch service provider.

HASM-1027

Message: `The secondary switch needs linecard power-cycle for the connector configuration to take effect.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that a static port breakout operation has completed and the line card (LC) needs to be power cycled for the changes to take effect.

Recommended Action: Power cycle the LC whose 40 Gigabit Ethernet port has been broken out by using the **`power-off linecard`** and **`power-on linecard`** commands for the changes to take effect.

HASM-1028

Message: `The secondary switch needs reload or linecard power-cycle for the port-group configuration to take effect.`

Message Type: LOG

Severity:INFO

Probable Cause: Indicates that a static port group operation has completed and the line card (LC) needs to be power cycled for the changes to take effect.

Recommended Action: Power cycle the linecard whose port group configuration has been changed to performance mode by using the **`power-off linecard`** and **`power-on linecard`** commands for the changes to take effect.

HASM-1029

Message: `The secondary switch needs to be rebooted for the new hardware profile configuration to take effect.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that the secondary node has taken on a new hardware profile configuration from primary database upon rejoining the cluster.

Recommended Action: The secondary switch need to be rebooted for the new profile configuration to take effect.

Execute the **`reload system`** command to reboot the secondary switch.

HASM-1030

Message: `Failed to find the custom KAP profile specified. Use the default KAP profile instead.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates failure to find the custom Keep-alive Protocol (KAP) profile specified in the user configuration. It will instead use the default KAP profile to boot up the switch.

Recommended Action: Verify the hardware KAP profile configuration. This is likely an error condition.

HASM-1105

Message: `Switch bring-up timed out.`

Message Type: FFDC | LOG

Severity: CRITICAL

Probable Cause: Indicates that the system timed out during a reload or sequence, waiting for one or more programs to register with system services or to fail over to active status.

Recommended Action: If the switch is in an inconsistent state, reload or power cycle the chassis. Before reloading the chassis, record the firmware version on the switch or management module and execute the **`ha dump`** command. If this is a dual-management module switch, gather the output from the management module in which this log message appeared.

HASM-1108

Message: `All service instances become active.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that all service instances became active. Active is an intermediate stage in the boot process.

Recommended Action: No action is required.

HASM-1109

Message: `The system is ready for configuration replay.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that all line cards (LCs) are online and the system is ready for configuration replay.

Recommended Action: No action is required.

HASM-1110

Message: `Configuration replay has completed on the system.`

Message Type:LOG

Severity: INFO

Probable Cause: Indicates that configuration replay has completed.

Recommended Action: No action is required.

HASM-1111

Message: `Configuration replay has completed on <slot/partition>.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that configuration replay has completed on the specified slot or partition.

Recommended Action: No action is required.

HASM-1120

Message: `Current version <firwmare version string>.`

Message Type: LOG |

Class: FIRMWARE

Severity: INFO

Probable Cause: Indicates the current firmware version string.

Recommended Action: No action is required.

HASM-1121

Message: `New version <firmware version string>.`

Message Type: LOG |

Class: FIRMWARE

Severity: INFO

Probable Cause: Indicates the new firmware version string after firmware download.

Recommended Action: No action is required.

HASM-1134

Message: `All service instances on Active.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that all service instances on Active.

Recommended Action: No action is required.

HASM-1200

Message: `Detected termination of process <Software component>:<Software component Process ID>.`

Message Type: FFDC | LOG

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.

HASM-1201

Message: `<Software component>:<Software component Process ID> failed to refresh (<Current time>:<Refresh time>, kill-<signal killed>).`

Message Type: FFDC | LOG

Severity: WARNING

Probable Cause: Indicates that one of the 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.

HASM-1202

Message: `Detected termination of hasmd process <HASM Process ID>.`

Message Type: FFDC | LOG

Severity: CRITICAL

Probable Cause: Indicates that the High Availability System Management (HASM) daemon has terminated unexpectedly.

Recommended Action: Copy the warning message along with any core file information and contact your switch service provider.

HIL Messages

HIL-1202

Message: `Blower <blower number> faulted, speed (<measured speed> RPM) below threshold.`

Message Type: LOG

Severity: ERROR

Probable Cause: Indicates that the specified fan speed (in RPMs) has fallen below the minimum threshold.

Recommended Action: Replace the fan field-replaceable unit (FRU). Refer to the Hardware Reference Manual of your switch for instructions to replace the fan FRU.

HIL-1301

Message:`A blower failed or missing. Replace failed or missing blower assembly immediately.`

Message Type: LOG

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 may overheat the switch.

Recommended Action: Replace the affected fan FRU immediately. Refer to the Hardware Reference Manual of your switch for instructions to replace the fan FRU

HIL-1302

Message: `<count> blowers failed or missing. Replace failed or missing blower assemblies immediately.`

Message Type: LOG

Severity: WARNING

Probable Cause: Indicates that multiple fan field-replaceable units (FRUs) have failed or are missing on the switch. This message is often preceded by a low fan speed message.

Recommended Action: Replace the affected fan FRUs immediately. Refer to the Hardware Reference Manual of your switch for instructions to replace the fan FRU.

HIL-1404

Message: `<count> fan FRUs missing. Install fan FRUs immediately.`

Message Type: LOG

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: `Current number of fans <good fans>, less than minimum of <minimum fans>. Shutdown in <seconds to shutdown> seconds. Replace fans immediately.`

Message Type: LOG

Severity: CRITICAL

Probable Cause: Indicates that one or more fan field-replaceable units (FRUs) have been removed.

Recommended Action: Install the missing fan FRUs immediately.

HIL-1406

Message: `Current number of fans <good fans>, less than minimum of <minimum fans>. Shutdown now!`

Message Type: LOG

Severity: CRITICAL

Probable Cause: Indicates that one or more fan field-replaceable units (FRUs) have been removed.

Recommended Action: Install the missing fan FRUs immediately.

HIL-1407

Message: `Shutdown cancelled!`

Message Type: LOG

Severity: WARNING

Probable Cause: Indicates that the current number of fans is now above the minimum and shutdown has been cancelled.

Recommended Action:

HIL-1408

Message: `PSU mismatch detected. Shutdown in <seconds to shutdown> seconds. Replace PSU immediately.`

Message Type: LOG

Severity: CRITICAL

Probable Cause: Indicates PSU airflow direction mismatch has been detected.

Recommended Action: Replace the mismatched PSU immediately.

HIL-1409

Message: `PSU mismatch detected. Shutdown now!`

Message Type: LOG

Severity: CRITICAL

Probable Cause: Indicates PSU airflow direction mismatch has been detected.

Recommended Action: Install the correct PSUs immediately.

HIL-1410

Message: `Shutdown cancelled!`

Message Type: LOG

Severity: WARNING

Probable Cause: Indicates PSU airflow direction mismatch has been resolved.

Recommended Action:

HIL-1505

Message: `High temperature (<measured temperature> C), fan speed increasing per environmental specifications.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that temperature in the system has risen above the warning threshold and the fan speed has been increased to prevent overheating of the system.

Recommended Action: Execute the **`show environment fan`** command to verify that all fans are working properly.

Make sure that the area is well ventilated and the room temperature is within operational range of your switch. Refer to the Hardware Reference Manual of 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

Severity: CRITICAL

Probable Cause: Indicates that temperature in the system has risen above the critical threshold.

Recommended Action: Execute the **`show environment fan`** 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 the room temperature is within operational range of your switch. Refer to the Hardware Reference Manual of your switch for the operational temperature range.

HIL-1510

Message: `Current temperature (<measured temperature> C) is below shutdown threshold. System shut down cancelled.`

Message Type: LOG

Severity: WARNING

Probable Cause: Indicates that temperature in the system has dropped below the critical threshold; the system will continue operation.

Recommended Action: To help prevent future problems, execute the **`show environment fan`** command to verify all fans are working properly.

Make sure that the area is well ventilated and the room temperature is within operational range of your switch. Refer to the Hardware Reference Manual of your switch for the operational temperature range.

HIL-1511

Message: `MISMATCH in Fan airflow direction. Replace FRU with fan airflow in same direction.`

Message Type: LOG

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-1512

Message: `MISMATCH in PSU-Fan FRUs airflow direction. Replace PSU with fan airflow in same direction.`

Message Type: LOG

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-1514

Message: `High temperature (<measured temperature> C) exceeds system temperature limit. System will shut down within 96 hours.`

Message Type: FFDC | LOG

Severity: CRITICAL

Probable Cause: Indicates that the temperature in the system has risen above the critical threshold.

Recommended Action: Execute the **`show environment fan`** 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 the room temperature is within operational range of your switch. Refer to the Hardware Reference Manual of your switch for the operational temperature range.

HIL-1515

Message: `High temperature (<measured temperature> C) exceeds system temperature limit. System will shut down in <time until shutdown>.`

Message Type: LOG

Severity: CRITICAL

Probable Cause: Indicates that the temperature in the system has risen above the critical threshold.

Recommended Action: Execute the **`show environment fan`** 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 the room temperature is within operational range of your switch. Refer to the Hardware Reference Manual of your switch for the operational temperature range.

HIL-1516

Message: `High temperature (<measured temperature> C) exceeds maximum system temperature limit. System will shut down immediately.`

Message Type: FFDC | LOG

Severity: CRITICAL

Probable Cause: Indicates that the temperature in the system has risen above the maximum threshold.

Recommended Action: Manually power cycle the system to recover. Execute the **`show environment fan`** 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 the room temperature is within operational range of your switch. Refer to the Hardware Reference Manual of your switch for the operational temperature range.

HIL-1517

Message: `MISMATCH in Fan <unit> airflow direction. Replace FRU with fan airflow in same direction.`

Message Type: LOG

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 FRUs.

HIL-1518

Message: `MISMATCH in PSU-Fan <unit> airflow direction. Replace PSU with fan airflow in same direction.`

Message Type: LOG

Severity: WARNING

Probable Cause: Indicates that the airflow of the power supply unit (PSU) is in the reverse direction. This may heat up the system.

Recommended Action: Replace the PSU fan field-replaceable units (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.

Make sure that the area is well ventilated and the room temperature is within operational range of your switch. Refer to the Hardware Reference Manual of your switch for the operational temperature range.

HIL-1521

Message: `<Slot Identifier>, high temperature (<measured temperature>).`

Message Type: LOG

Severity: WARNING

Probable Cause: Indicates that the temperature of the specified interface module has risen above the warning threshold.

Recommended Action: Execute the **`show environment fan`** command to verify that all 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 of your switch for the operational temperature range.

HIL-1522

Message: `<Slot Identifier>, high temperature (<measured temperature>). Unit will be shut down in 2 minutes if temperature remains high.`

Message Type: FFDC | LOG

Severity: CRITICAL

Probable Cause: Indicates that the temperature of the specified interface module has risen above the critical threshold. This usually follows a high temperature message.

Recommended Action: Execute the **`show environment fan`** command to verify that all fans are working properly.

Make sure that the area is well ventilated and the room temperature is within operational range of your switch. Refer to the Hardware Reference Manual of your switch for the operational temperature range.

If the message persists, replace the interface module.

HIL-1523

Message: `<Slot Identifier>, unit shutting down.`

Message Type: FFDC | LOG

Severity: CRITICAL

Probable Cause: Indicates that the temperature of the specified interface module was above the maximum threshold for at least two minutes and therefore it has been shut down to prevent damage. This message usually follows a high temperature warning message.

Recommended Action: Execute the **`show environment fan`** command to verify that all fans are working properly.

Make sure that the area is well ventilated and the room temperature is within the operational range of your switch. Refer to the Hardware Reference Manual of your switch for the operational temperature range.

If the message persists, replace the faulty interface module.

HIL-1524

Message: `<Slot Identifier> is below shutdown threshold. Blade shut down cancelled.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that the temperature of the specified interface module has dropped below the critical threshold; the system will continue operation.

Recommended Action: To help prevent future problems, execute the **`show environment fan`** command to verify that all fans are working properly.

Make sure that the area is well ventilated and the room temperature is within operational range of your switch. Refer to the Hardware Reference Manual of your switch for the operational temperature range.

HIL-1531

Message: `Temperature sensor ID=<sensor-id> value=<measured temperature>C Transitioned from <old-state> to <new-state>`

Message Type:LOG

Severity:INFO

Probable Cause: Informs about normal change of temperature recorded by the particular sensor. Usually, this message is generated for the following temperature transitions:

- Alarm to Normal
- Critical to Normal

Recommended Action: None

HIL-1532

Message: `Temperature sensor ID=<sensor-id> value=<measured temperature>C Transitioned from <old-state> to <new-state>`

Message Type:LOG

Severity:WARNING

Probable Cause: Warns about a change of temperature recorded by the particular sensor. Usually, this message is generated for the following temperature transitions:

- Normal to Alarm
- Critical to Alarm

Recommended Action: To help prevent future problems, execute the **`show environment fan`** command to verify all fans are working properly.

Make sure that the area is well ventilated and the room temperature is within operational range of your switch. Refer to the Hardware Reference Manual of your switch for the operational temperature range.

HIL-1533

Message: `Temperature sensor ID=<sensor-id> value=<measured temperature>C Transitioned from <old-state> to <new-state>`

Message Type:LOG

Severity: CRITICAL

Probable Cause: Warns about a critical change of temperature recorded by the particular sensor. Usually, this message is generated for the following temperature transitions:

- Normal to Critical
- Alarm to Critical

Recommended Action: To help prevent future problems, execute the **`show environment fan`** command to verify all fans are working properly.

Make sure that the area is well ventilated and the room temperature is within operational range of your switch. Refer to the Hardware Reference Manual of your switch for the operational temperature range.

HIL-1605

Message: `High temperature (<measured temperature> C), fan speed increasing per environmental specifications.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that temperature in the system has risen above the threshold and therefore the fan speed has been increased to prevent overheating of the system.

Recommended Action: No action is required.

HIL-1700

Message: `Fan speed changing due to optics thermal monitoring. Status: <Optics Status>`

Message Type: LOG

Severity: WARNING

Probable Cause: Indicates that optics temperatures in the system have risen above the warning threshold and that the fan speed is being increased.

Recommended Action: Run the **`show environment fan`** 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-1701

Message: `All optics are now below the thermal warning threshold. Fan speed will resume as per thermal policy.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that optics temperatures in the system are now below the warning threshold and that the fan speed is returning to the speed dictated by the switch thermal policy.

Recommended Action: Run the **`show environment fan`** command to verify all fans are working properly.

HSL Messages

HSL-1000

Message: `HSL initialization failed.`

Message Type: LOG

Severity: CRITICAL

Probable Cause: Indicates a hardware subsystem layer (HSL) initialization failure. This error is caused by other system errors.

Recommended Action: Execute the **`copy support`** command and contact your switch service provider.

HSL-1001

Message:`Failed to acquire the system MAC address pool.`

Message Type: LOG

Severity: CRITICAL

Probable Cause: Indicates the failure to acquire the system address. This error is caused by other system errors.

Recommended Action: Execute the **`show logging raslog`** command to view the error log for other system errors and correct the errors.

HSL-1004

Message: `Incompatible SFP transceiver for interface <InterfaceName> is detected.`

Message Type: LOG

Severity: ERROR

Probable Cause: Indicates that an incompatible small form-factor pluggable (SFP) transceiver for the interface has been inserted.

Recommended Action: Disable the interface using the shutdown command and insert an SFP transceiver that is supported on the interface. After the SFP transceiver is inserted, re-enable the interface using the **no shutdown** command

HSL-1006

Message: `Failed to get the kernel page size <PageSize> bytes for the Memory Map (MMap).`

Message Type: LOG

Severity: CRITICAL

Probable Cause: Indicates that there is not enough contiguous kernel memory.

Recommended Action: Execute the **show logging raslog** command to view the error log for other system errors and correct the errors.

HSL-1009

Message: `Failed to create Extreme trunk interface <InterfaceName>.`

Message Type: LOG

Severity: ERROR

Probable Cause: Indicates failure to create Extreme trunk because the hardware resources are exhausted.

Recommended Action: Do not exceed the maximum trunk configuration allowed by the system.

HSL-1010

Message: `Reached max VRBIDs usage, VRB-ID allocation failed in ASIC.`

Message Type: LOG

Severity: ERROR

Probable Cause: Indicates that maximum VRBIDs have been used.

Recommended Action: No action is required.

HSL-1011

Message: `Resource limit reached, <Number of resources to be freed.> resources are required for the virtual-fabric entry.`

Message Type: LOG

Severity: ERROR

Probable Cause: Indicates that maximum resources have been used.

Recommended Action: No action is required.

HSL-1020

Message: `interface <InterfaceName> received remote fault.`

Message Type: LOG

Severity: ERROR

Probable Cause: Indicates interface has received a remote fault from peer.

Recommended Action: No action is required.

HSL-1021

Message: `interface <InterfaceName> detected local fault.`

Message Type: LOG

Severity: ERROR

Probable Cause: Indicates interface has detected a local fault.

Recommended Action: No action is required.

HSL-1022

Message: `Remote fault cleared on interface <InterfaceName>.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates remote fault is cleared on interface.

Recommended Action: No action is required.

HSL-1023

Message: `Local fault cleared on interface <InterfaceName>.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates local fault is cleared on interface.

Recommended Action: No action is required.

HSL-1024

Message: `Optic inserted in interface <InterfaceName> is not Extreme branded.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates optic is not Extreme branded.

Recommended Action: No action is required.

HSL-1025

Message: `Optic inserted in interface <InterfaceName> is not compatible.`

Message Type: LOG

Severity: WARNING

Probable Cause: Indicates optic is not compatible with current port configuration.

Recommended Action: No action is required.

HSL-1026

Message: `FEC Resources on LC: <linecardid> unit: <unit> are exhausted. Time since last log <current_time> and total fail count: <fail_count>.`

Message Type: LOG

Severity: WARNING

Probable Cause: Indicates FEC resources are exhausted on the unit of line card.

Recommended Action: No action is required.

HSL-1027

Message: `Service Port link is UP/Down`

Message Type: LOG

Severity: INFO

Probable Cause: When Service Port link is Changed by up to down and vice-versa.

Recommended Action: No action is required.

HSL-1028

Message: `Offline Diagnostic Test on <lc_sfm_type>: <linecardid> status: <log_status> [<result_updated>].`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates status for Offline Diagnostic Test for a line card / SFM.

Recommended Action: No action is required.

HSL-1029

Message: `Offline Diagnostic Test on file no found on <lc_sfm_type>: <linecardid>.`

Message Type: LOG

Severity: WARNING

Probable Cause: Indicates Offline Diagnostic Test file not present on a line card / SFM.

Recommended Action: No action is required.

HSL-1030

Message: `Offline Diagnostic Test on <lc_sfm_type>: <linecardid> status: <log_status> [<result_updated>].`

Message Type: LOG

Severity: CRITICAL

Probable Cause: Indicates failure status for Offline Diagnostic Test for a line card / SFM.

Recommended Action: No action is required.

HSL-1031

Message: `Optic inserted in interface <InterfaceName> is not compatible and laser is disabled.`

Message Type: LOG

Severity: ERROR

Probable Cause: Indicates optic is not compatible with current port configuration.

Recommended Action: No action is required.

HSL-1032

Message: `<msg>`

Message Type: LOG

Severity: INFO

Probable Cause: None

Recommended Action: None.

HSL-1033

Message: `Temperature of optic inserted in interface <InterfaceName> is above critical threshold and it is put in reset.`

Message Type: LOG

Severity: CRITICAL

Probable Cause: Indicate the optic temperature in the cage is over critical threshold

Recommended Action: Replace a new optic and do shut/no shut on the port.

HSL-1034

Message: `Temperature of optic inserted in interface <InterfaceName> is above warning threshold.`

Message Type: LOG

Severity: WARNING

Probable Cause: Indicates that the optic temperature in the specified interface is over warning threshold.

Recommended Action: Replace a new optic and do shut/no shut on the port.

HSL-1052

Message: `fec mode <RS-FEC | FC-FEC | Auto-Negotiation | Disabled>`

Message Type: LOG

Severity: ERROR

Probable Cause: This message is generated when an unsupported FEC mode is configured on an interface with 25G optics. The affected interface is identified in the message.

Recommended Action: Confirm the supported FEC modes for the optic in question with the Release Notes. Verify that the optic is configured for the appropriate FEC mode. If you attempt

to configure any mode other than a supported mode for that optic, then an Error Message will be generated.

HSL-1061

Message: `{NexthopTable|RouteTable|HostTable|ECMPTable|EncapTable} reached the high threshold limit of {high-threshold-level}.`

Message Type: WARNING

Severity: WARNING

Probable Cause: One of the following 5 tables has reached the user configured low threshold level.

- NextHopTable
- RouteTable
- HostTable
- ECMPTable
- EncapTable

Recommended Action: Reduce the size of the Next Hop Table or Route Table.

HSL-1062

Message: `{NexthopTable|RouteTable|HostTable|ECMPTable|EncapTable} reached the low threshold limit of {low-threshold-level}.`

Message Type: WARNING

Severity: WARNING

Probable Cause: One of the following 5 tables has reached the user configured low threshold level.

- NextHopTable
- RouteTable
- HostTable
- ECMPTable
- EncapTable

Recommended Action: No action is required.

HSL-1069

Message: `MAC collision occurred in HW for MAC:[{mac-address}], VlanId/BDId:{vlan-id|bd-id} ({V|B})`

Message Type: ERROR

Severity: ERROR

Probable Cause: MAC Collision detected.

Recommended Action: No action is required.

HSL-1070

Message: `HW BFD thread has stopped unexpectedly. SLX will automatically reload to restore the BFD functionality.`

Message Type: LOG

Severity: CRITICAL

Probable Cause: The hardware BFD thread has stopped unexpectedly.

Recommended Action: None. The device will reload automatically to restore BFD.

HSL-1071

Message: `I2C errors found in accessing CPLD for the port <port-number> and it may be shutdown. Reboot the device to recover.`

Message Type: LOG

Severity: WARNING

Probable Cause: I2C error while accessing CPLD.

Recommended Action: Reboot the device to recover.

HSL-1072

Message: `I2C errors found in accessing the EEPROM for the port <port-number> and it may be shutdown. Remove and/or replace pluggable media on this port and reboot the device to recover.`

Message Type: LOG

Severity: WARNING

Probable Cause: I2C error while accessing the EEPROM of the media.

Recommended Action: Remove and/or replace the pluggable media on this port and reboot the device to recover.

IGMP Messages

IGMP-1001

Message:`MsgQ enqueue failed (rc: <rc>).`

Message Type: DCE

Severity: ERROR

Probable Cause: Indicates an internal inter-process communication (IPC) failure due to the scalability scenario.

Recommended Action: Reduce the number of groups and MRouter ports.

IGMP-1002

Message: `IPC with McastSS failed (message-id: <message-id>, rc: <rc>).`

Message Type: DCE

Severity: ERROR

Probable Cause: Indicates an internal inter-process communication (IPC) failure due to the scalability scenario.

Recommended Action: Reduce the number of groups and MRouter ports.

IGMP-1004

Message: `IGMP maximum VLANs enabled. Cannot enable IGMP on <vlan>.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that the number of VLANs on which Internet Group Multicast Protocol (IGMP) can be enabled has reached the maximum limit. Therefore, IGMP cannot be enabled on the specified VLAN.

Recommended Action: No action is required.

IGMP-1005

Message: `IGMP snooping enabled on total <vlan> VLANs. Maximum limit reached.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that the number of VLANs on which Internet Group Multicast Protocol (IGMP) can be enabled has reached the maximum limit.

Recommended Action: No action is required.

IGMP-1006

Message: `IGMP snooping enabled on <vlan>.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that the Internet Group Multicast Protocol (IGMP) is enabled on a particular VLAN.

Recommended Action: No action is required.

IPAD Messages

IPAD-1000

Message:

```
IP Config change: Entity:<Type of managed entity>/<Instance number of
managed entity> Interface:<Type of network interface> <Instance Index
of network interface> Adresss family:<Protocol address family> Source of
change:<Source of address change> Address:<Value of address and prefix>
DHCP:<DHCP enabled or not>.
```

Message Type: LOG

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.

Recommended Action: No action is required.

IPAD-1001

Message:`<Type of managed entity>/<Instance number of managed entity> <Protocol address family> <Source of address change> <Value of address> DHCP <DHCP enabled or not>.`

Message Type: LOG

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.

Recommended Action: No action is required.

IPAD-1002

Message: `Switch name has been successfully changed to <Switch name>.`

Message Type: LOG | AUDIT

Class: CFG

Severity: INFO

Probable Cause: Indicates that the switch name has been changed.

Recommended Action: No action is required.

IPAD-1003

Message: `libipadm: <error message> <error message specific code>.`

Message Type: LOG | FFDC

Severity: ERROR

Probable Cause: Indicates that the IP admin library has encountered an unexpected error.

Recommended Action: Execute the copy support command and contact your switch service provider.

IPAD-1004

Message: `Unable to set the host name due to /etc/hosts file corruption.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that the /etc/hosts file was inconsistent and it could not be recovered.

Recommended Action: Execute the copy support command and contact your switch service provider.

IPAD-1005

Message: `The /etc/hosts file was inconsistent but has been recovered successfully.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that the /etc/hosts file was inconsistent but it was recovered.

Recommended Action: No action is required.

IPAD-1006

Message: `Chassis name has been successfully changed to <Chassis name>.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that the chassis name has been changed.

Recommended Action: No action is required.

IPHL Messages

IPHL-1001

Message: `Interface has only anycast IP. Please configure the DHCP gateway interface IP`

Message Type: DCE

Class: NONE

Severity: WARNING

Probable Cause: If only anycast IP is configured, DHCP Relay packets may not land on the same leaf in an IP Fabric

Recommended Action: Configure the gateway IP using the `ip dhcp relay gateway interface` command with appropriate options

IPHL-1002

Message: `Received DHCP Client packet (<DHCP Packet Type>) with option82 but option82 allow untrusted is disabled`

Message Type: DCE

Class: NONE

Severity: WARNING

Probable Cause: Allow option82 on untrusted port is not enabled

Recommended Action: For client packets with Opt82 info, enable option allow untrusted configuration

IPHL-1003

Message: `No valid trusted interface on vlan <VLAN ID>. Received <DHCP Packet Type> packet on client interface <Client Facing Interface>`

Message Type: DCE

Class: NONE

Severity: WARNING

Probable Cause: No trusted DHCP server facing interface

Recommended Action: configure trust on server facing interface

IPHL-1004

Message:`No binding entry found for <DHCP Packet Type> packet on vlan <VLAN ID> IP <IP Address> MAC<MAC Address>`

Message Type: DCE

Class: NONE

Severity: WARNING

Probable Cause: No binding entry found in the dhcp snooping binding database

Recommended Action: NONE

IPHL-1005

Message: `<DHCP Packet Type> packet received on invalid interface <Received Interface>. Binding entry vlan <VLAN ID>IP <IP Address> MAC <MAC Address> interface <Binding Interface>`

Message Type: DCE

Class: NONE

Severity: WARNING

Probable Cause: Packed received on interface does not match with interface present in binding entry

Recommended Action: verify interface on which packet was received

IPHL-1006

Message: `DHCP packet from server received on untrusted port <Received Interface> vlan <VLAN ID>`

Message Type: DCE

Class: NONE

Severity: WARNING

Probable Cause: Packed received on an untrusted port

Recommended Action: verify the port on which packet was received

IPHL-1007

Message: `DHCPv6: Maximum allowed <Maximum Delegated Prefix Value> delegated prefixes learned on interface <Interface Name>`

Message Type: DCE

Class: NONE

Severity: WARNING

Probable Cause: Reached maximum allowed delegated prefixes on the interface

Recommended Action: NONE

IPHL-1008

Message: `DHCPv6: Maximum allowed <Maximum Delegated Prefix Value> delegated prefixes learned on system`

Message Type: DCE

Class: NONE

Severity: WARNING

Probable Cause: Reached maximum allowed delegated prefixes on the system

Recommended Action: NONE

KTRC Messages

KTRC-1001

Message: `Dump memory size exceeds dump file size.`

Message Type: LOG

Severity: WARNING

Probable Cause: Indicates that the dump memory size has exceeded the dump file size.

Recommended Action: Execute the copy support command and reload the switch. If the problem persists, contact your switch service provider.

KTRC-1002

Message:`Concurrent trace dumping.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that the initial background dump has not completed.

Recommended Action: No action is required.

KTRC-1003

Message: `Cannot open ATA dump device.`

Message Type: LOG

Severity: ERROR

Probable Cause: Indicates that the advanced technology attachment (ATA) dump driver is not initialized properly.

Recommended Action: Execute the copy support 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

Severity: ERROR

Probable Cause: Indicates that the write boundary in the advanced technology attachment (ATA) dump device has been exceeded.

Recommended Action: Execute the copy support 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

Severity: ERROR

Probable Cause: Indicates that trace was unable to initialize.

Recommended Action: Execute the copy support command and reload the switch. If the problem persists, contact your switch service provider.

L2AG Messages

L2AG-1001

Message:`Linux socket error - error reason: <reason>, socket name: <sockname>, error name<errorname>.`

Message Type: DCE

Severity: ERROR

Probable Cause: Indicates that an error has occurred in the Linux socket.

Recommended Action: Reload or power cycle the switch.

L2AG-1002

Message: `Initialization error : <reason>.`

Message Type: DCE

Severity: ERROR

Probable Cause: Indicates that the Layer 2 Agent (L2AGT) has encountered an error during initialization.

Recommended Action: Reload or power cycle the switch.

L2AG-1003

Message: `Message Queue Error : Message queue create failed.`

Message Type: DCE

Severity: ERROR

Probable Cause: Indicates that the Layer 2 Agent (L2AGT) has encountered system service manager (SSM) message queue errors.

Recommended Action: Reload or power cycle the switch.

L2AG-1004

Message: `FDB error: Error in creating AVL tree.`

Message Type: DCE

Severity: ERROR

Probable Cause: Indicates that the Layer 2 Agent (L2AGT) has encountered an error while initializing the AVL tree.

Recommended Action: Reload or power cycle the switch.

L2AG-1005

Message: `MAC-address-table hash failed even after two attempts for slot <slot> chip <chip>.`

Message Type: DCE

Severity: ERROR

Probable Cause: Indicates that the media access control (MAC) address table hash failed even after two hash changes on the specified chip.

Recommended Action: Reload or power cycle the switch.

L2AG-1006

Message: `MAC-address-table on slot <Slot_id> chip <Chip_id> is 95 percent full.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that the media access control (MAC) address table on the chip is 95 percent full.

Recommended Action: Clear some of the entries using the **`clear mac-address-table dynamic`** command or wait until the old entries age out.

L2AG-1007

Message: `MAC-address-table on slot <Slot_id> chip <Chip_id> is less than 90 percent full.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that the media access control (MAC) address table is less than 90 percent full.

Recommended Action: No action is required. The Layer 2 Agent (L2AGT) will start learning the entries.

L2AG-1008

Message: `MAC-address-table on slot <Slot_id> chip <Chip_id> is 95 percent full [Dynamic/Static MAC's: <fdb_count>; ACL MAC's: <Acl_count>].`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that the media access control (MAC) address table on the chip is 95 percent full.

Recommended Action: Clear some of the entries using the **clear mac-address-table dynamic** command or wait until the old entries age out.

L2AG-1009

Message: `L2 H/W tables have reached capacity. Few ACL/MAC entries may not be configured in H/W, resulting in flooding.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that some of the Layer 2 hardware tables are full.

Recommended Action: Clear some of the entries using the **clear mac-address-table dynamic** command or wait until the old entries age out.

L2AG-1010

Message: `ERROR: Mac Vlan Classification table is Full. Add Failed for Vlan <ivid> Mac <mac1>:<mac2>:<mac3>:<mac4>:<mac5>:<mac6> on <ifname>.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that the Layer 2 classifier hardware table is full.

Recommended Action: Remove the existing MAC VLAN entries and reconfigure.

L2AG-1011

Message: `Mgr-Agt Checksum Mismatch reached the threshold for Slot:<slot-id>. Requesting the MAC Refresh from L2 Manager.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that the MAC entries may be out of synchronization between the Layer 2 Manager and the Layer 2 Agent.

Recommended Action: No action is required.

L2SS Messages

L2SS-1001

Message: `Linux socket error - error reason: <reason>, socket name: <sockname>, error name <errorname>.`

Message Type: DCE

Severity: ERROR

Probable Cause: Indicates that an error has occurred in the Linux socket.

Recommended Action: Reload or power cycle the switch.

L2SS-1002

Message: `Initialization error: <reason>.`

Message Type: DCE

Severity: ERROR

Probable Cause: Indicates that the Layer 2 system (L2SYS) has encountered an error during initialization.

Recommended Action: Reload or power cycle the switch.

L2SS-1003

Message: `Message Queue Error: Failed to create a Message Queue.`

Message Type: DCE

Severity: ERROR

Probable Cause: Indicates that the Layer 2 system (L2SYS) has encountered system service manager (SSM) message queue errors.

Recommended Action: Reload or power cycle the switch.

L2SS-1004

Message: `FDB error: Error in creating the AVL tree.`

Message Type: DCE

Severity: ERROR

Probable Cause: Indicates that the Layer 2 system (L2SYS) has encountered an error while initializing the AVL tree.

Recommended Action: Reload or power cycle the switch.

L2SS-1005

Message: `MAC-address-table hash failed even after two attempts for slot <slot> chip <chip>.`

Message Type: DCE

Severity: ERROR

Probable Cause: Indicates that the media access control (MAC) address table hash failed even after two hash changes on the specified chip.

Recommended Action: Reload or power cycle the switch.

L2SS-1008

Message: `Adding Internal MAC <mac1>:<mac2>:<mac3>:<mac4>:<mac5>:<mac6> VID <Vid> as a static MAC.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that a static media access control (MAC) is overriding an internal MAC entry (VRRP/SVI).

Recommended Action: No action is required.

L2SS-1009

Message: `Fabric-wide Layer 2 flush command issued.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that a fabric-wide Layer 2 flush command is issued and the entire Layer 2 forwarding table will be cleared.

Recommended Action: No action is required.

L2SS-1010

Message: `Fabric-wide l2 flush completed, status - <command status>.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that the entire Layer 2 forwarding table has been cleared.

Recommended Action: No action is required.

L2SS-1011

Message: `Security violation occured on interface <Ifname> with Mac <mac1><mac2>.<mac3><mac4>.<mac5><mac6> Vlan <vid>.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that the number of Media Access Control (MAC) addresses allowed on the specified interface has reached the maximum limit. Based on the configured action, the interface is either shut down or the MAC learning is restricted.

Recommended Action: No action is required.

L2SS-1012

Message: `Failed to create Tunnel <Ifid>.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that tunnel creation was unsuccessful.

Recommended Action: Technical support is required.

L2SS-1013

Message: `Failed to delete Tunnel <Ifid>.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that tunnel deletion was unsuccessful.

Recommended Action: Technical support is required.

L2SS-1014

Message: `Failed to handle Tunnel-Vlan association, Tunnel <Ifid> not found.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that tunnel VLAN association handling was unsuccessful.

Recommended Action: Technical support is required.

L2SS-1015

Message: `Failed to handle Tunnel-Vlan disassociation, Tunnel <Ifid> not found.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that tunnel VLAN disassociation handling was unsuccessful.

Recommended Action: Technical support is required.

L2SS-1016

Message: `Failed to associate Tunnel <Ifid> to Vlan <Vid>, Vlan not present.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that tunnel VLAN association was unsuccessful.

Recommended Action: Technical support is required.

L2SS-1017

Message: `Failed to disassociate Tunnel <Ifid> from Vlan <Vid>, Vlan not present.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that tunnel VLAN disassociation was unsuccessful.

Recommended Action: Technical support is required.

L2SS-1018

Message: `Failed to configure Remote VM MAC <mac1><mac2>.<mac3><mac4>.<mac5><mac6> for Tunnel <ifid> on Vlan <vid>.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that configuring remote Virtual Machine (VM) Media Access Control (MAC) on the tunnel was unsuccessful.

Recommended Action: Technical support is required.

L2SS-1019

Message: `Failed to remove Remote VM MAC <mac1><mac2>.<mac3><mac4>.<mac5><mac6> for Tunnel <ifid> on Vlan <vid>.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that removing remote Virtual Machine (VM) Media Access Control (MAC) on the tunnel was unsuccessful.

Recommended Action: Technical support is required.

L2SS-1020

Message: `MAC move detected across interface(s) <InterfaceList> for MAC <mac1>:<mac2>:<mac3>:<mac4>:<mac5>:<mac6>, VLAN <Vlan ID>.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that the MAC address is flapping across multiple interfaces.

Recommended Action: No action is required.

L2SS-1021

Message: `Rate limiting frequent MAC move detection logs. No more logs will be reported.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that MAC move logging has been stopped to avoid flooding.

Recommended Action: Use "mac-move-detect log reset-count" to know if MAC moves are still happening

L2SS-1022

Message: `MAC move detection and Virtual fabric can not co-exist. Disabling MAC move.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that Virtual fabric was enabled after enabling MAC move detection.

Recommended Action: Disable Virtual fabric to enable MAC move detection again.

L2SS-1024

Message: `Repeated mac move detected for Mac <mac1><mac2>.<mac3><mac4>.<mac5><mac6> Vlan <vid>, interface <Ifname> shut down.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates port shut down due to repeated mac move.

Recommended Action: No action is required.

L2SS-1025

Message: `Shut down recovery for interface <interface>`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates port shut recover due to multiple ports getting shut.

Recommended Action: No action is required.

L2SS-1026

Message: `Loop Detection (ELD) has triggered mac-address-table refresh`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that Edge Loop Detection (ELD) has detected loop and triggered mac-address-table refresh.

Recommended Action: No action is required.

L2SS-1027

Message: `Edge Loop Detection (ELD) has triggered mac-address-table refresh for interface <interface>`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that Edge Loop Detection (ELD) has detected loop and triggered mac-address-table refresh for specified interface.

Recommended Action: No action is required.

L2SS-1028

Message: `Duplicate MCT Static MAC addresses are identified.`

Message Type: DCE

Severity: ERROR

Probable Cause: Indicates that Between MCT Nodes duplicate static macs found .

Recommended Action: Delete the Duplicate MAC one of the MCT Node.

L2SS-1029

Message: `Duplicate static VPLS Mac <mac1>02x<mac2>02x.<mac3>02x<mac4>02x.<mac5>02x<mac6>02x is detected in bridge-domain <vid> on logical-interface <Ifname>.`

Message Type: DCE

Severity: ERROR

Probable Cause: Indicates that duplicate vpls static mac is configured in bridge-domain.

Recommended Action: Delete the latest Duplicate static MAC configured.

L2SS-1031

Message: `MAC-address-table has reached 100 percent full.`

Message Type: DCE

Severity: INFO

Probable Cause: MAC Address Table is full (100% capacity is used).

Recommended Action: No action is required.

L2SS-1036

Message: `MAC-address-table has reached the high threshold limit of %d percent.`

Message Type: DCE

Severity: INFO

Probable Cause: MAC Address Table has reached the user configured high threshold level. The configured value is displayed in the *%d* parameter.

Recommended Action: Clean up the MAC Address Table.

L2SS-1037

Message: `MAC-address-table has dropped below the low threshold limit of %d percent.`

Message Type: DCE

Severity: INFO

Probable Cause: MAC Address Table has dropped below the user configured low threshold level. The configured value is displayed in the *%d* parameter.

Recommended Action: No action is required

LACP Messages

LACP-1001

Message:`<module> Error opening socket (<error>).`

Message Type: DCE

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 version using the **`firmware download`** command.

LACP-1002

Message: `<Component> Initialization failed.`

Message Type: DCE

Severity: ERROR

Probable Cause: Indicates that an error occurred in the Link Aggregation Control Protocol (LACP) daemon.

Recommended Action: Take action specific to the error message.

LACP-1003

Message: `Port-channel <PortChannelKey> up in defaulted state.`

Message Type: DCE

Severity: INFO

Probable Cause:

Recommended Action: No action required.

LACP-1004

Message: `Port-channel <PortChannelKey> down from defaulted state.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that the specified port channel is down from the defaulted state.

Recommended Action: No action required.

LACP-1005

Message: `LACP <LinkName>:Could be a SSPA mismatch: New Actor Port <PduActorPort>, Old Actor Port <LinkPartnerPort>, New Partner Port: <PduPartnerPort> , Old Partner Port: <LinkActorPort>`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that wrong PDU is trapped a wrong port.

Recommended Action: No action required.

LACP-1006

Message: `LACP <LinkName>: MUX state transition <Str 1> to <Str 2><Str 3>`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that PDU are not received on expected interval

Recommended Action: No action required.

LIC Messages

LIC-1001

Message: `Out of memory in module <Function name>.`

Message Type: LOG

Severity: CRITICAL

Probable Cause: Indicates that an unexpected internal memory allocation failure has occurred.

Recommended Action: Try the operation again. If this operation fails, reload or fail over the switch.

LIC-1002

Message: `License is needed in linecard <Slot>.`

Message Type: LOG

Severity: ERROR

Probable Cause: Indicates that an License is not installed in the LC.

Recommended Action: Remove the config for the feature(s) for which license is required and power cycle the LC.

LIC-1003

Message: `License:<String> added to slot:<Number>.`

Message Type: LOG

Severity: INFO

Probable Cause:

Recommended Action:

LIC-1004

Message: `License:<String> removed from slot:<Number>.`

Message Type: LOG

Severity: INFO

Probable Cause:

Recommended Action:

LIC-1005

Message: `License EULA accepted for <Feature> feature.`

Message Type: LOG

Severity: INFO

Probable Cause: User has accepted usage of feature using Self Authenticated Upgrade .

Recommended Action:

LIC-1006

Message: `License EULA declined for <Feature> feature.`

Message Type: LOG

Severity: INFO

Probable Cause: User has declined usage of feature using Self Authenticated Upgrade.

Recommended Action:

LIC-1015

Message: Failed to read License Identifier from hardware. Licenses will be invalid. (error code=<Number>)

Message Type: LOG

Severity: CRITICAL

Probable Cause: Indicates that access to World Wide Name (WWN) card has failed.

Recommended Action: Reload or power cycle the switch, or replace the platform hardware.

LOG Messages

LOG-1000

Message: `Previous message has repeated <repeat count> times.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that the previous message was repeated the specified number of times.

Recommended Action: No action is required.

LOG-1001

Message:`A log message was dropped.`

Message Type: LOG | FFDC

Severity: WARNING

Probable Cause: Indicates that a log message was dropped. A trace dump file has been created.

Recommended Action: Execute the **`copy support`** command and contact your switch service provider.

LOG-1002

Message: `A log message was not recorded.`

Message Type: LOG

Severity: WARNING

Probable Cause: Indicates that a log 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 **`copy support`** command and contact your switch service provider.

LOG-1003

Message: `SYSTEM error log has been cleared.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that the persistent system error log has been cleared.

Recommended Action: No action is required.

LOG-1004

Message: `Log message <Log message that has been blocked> flooding detected and blocked.`

Message Type: LOG

Severity: WARNING

Probable Cause: Indicates that the specified message has been flooding and was blocked.

Recommended Action: Reload the switch. If the message persists, execute the **copy support** 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

Class: RAS

Severity: INFO

Probable Cause: Indicates that the specified message has been disabled from logging.

Recommended Action: No action is required.

LOG-1006

Message: `Log message <Log message that has been enabled> has been enabled.`

Message Type:AUDIT | LOG

Class: RAS

Severity: INFO

Probable Cause: Indicates that the specified message has been enabled for logging.

Recommended Action: No action is required.

LOG-1007

Message: `DCE error log has been cleared.`

Message Type:DCE

Severity: INFO

Probable Cause: Indicates that the persistent DCE error log has been cleared.

Recommended Action: No action is required.

LOG-1008

Message: `Log Module <Log Module that has been disabled> has been disabled.`

Message Type:AUDIT | LOG

Class: RAS

Severity: INFO

Probable Cause: Indicates that the specified module has been disabled from logging.

Recommended Action: No action is required.

LOG-1009

Message: `Log Module <Log Module that has been enabled> has been enabled.`

Message Type:AUDIT | LOG

Class: RAS

Severity: INFO

Probable Cause: Indicates that the specified module has been enabled for logging.

Recommended Action: No action is required.

LOG-1010

Message: `Internal Log message <Log message that has been enabled to be sent to syslog server> has been enabled for syslog logging.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that the specified message has been enabled for syslog logging.

Recommended Action: No action is required.

LOG-1011

Message: `Internal Log message <Log message that has been disabled from being sent to syslog server> has been disabled from syslog logging.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that the specified message has been disabled from syslog logging.

Recommended Action: No action is required.

LOG-1012

Message: `Log Message <Log Message Id> severity has been changed to <Severity>.`

Message Type: AUDIT | LOG

Class: RAS

Severity: INFO

Probable Cause: Indicates that the severity level of the specified log message has been changed.

Recommended Action: No action is required.

MAPS Messages

MAPS-1001

Message:`<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.`

Message Type: LOG

Severity: CRITICAL

Probable Cause: Indicates that the specified rule has been triggered because the errors are above the configured threshold.

Recommended Action: No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

MAPS-1002

Message: `<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.`

Message Type: LOG

Severity: ERROR

Probable Cause: Indicates that the specified rule has been triggered because the errors are above the configured threshold.

Recommended Action: No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

MAPS-1003

Message: `<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.`

Message Type: LOG

Severity: WARNING

Probable Cause: Indicates that the specified rule has been triggered because the errors are above the configured threshold.

Recommended Action: No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

MAPS-1004

Message: <object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that the specified rule has been triggered because the errors are above the configured threshold.

Recommended Action: No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

MAPS-1010

Message: `Port(s) fenced due to RuleName=<Rule name>, Condition=<condition>, Obj:<object> <ms, values, units>.`

Message Type: LOG

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

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

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-1020

Message: `Switch wide status has changed from <Previous state> to <Current state>.`

Message Type: LOG | AUDIT

Class: MAPS

Severity: WARNING

Probable Cause: Indicates that the switch is not in a healthy state. This occurred because of a rule violation.

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

Class: MAPS

Severity: WARNING

Probable Cause: Indicates that the switch status has changed to a healthy state. This occurred because none of the factors are violated.

Recommended Action: No action is required.

MAPS-1100

Message: `Rule <Rule name> is created.`

Message Type: LOG | AUDIT

Class: MAPS

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

Class: MAPS

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

Class: MAPS

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

Class: MAPS

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

Class: MAPS

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

Class: MAPS

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

Class: MAPS

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

Class: MAPS

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

Class: MAPS

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

Class: MAPS

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

Class: MAPS

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

Class: MAPS

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

Class: MAPS

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

Class: MAPS

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

Class: MAPS

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

Class: MAPS

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

Class: MAPS

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

Class: MAPS

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

Class: MAPS

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

Class: MAPS

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> has resumed.`

Message Type: LOG | AUDIT

Class: MAPS

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-1200

Message: `Fabric Watch Thresholds are converted to MAPS policies.`

Message Type: LOG | AUDIT

Class: MAPS

Severity:INFO

Probable Cause: Indicates that the current Fabric Watch configuration has converted to corresponding MAPS policies.

Recommended Action: Verify the MAPS policies and make sure the rules are valid before enabling MAPS.

MAPS-1201

Message: `MAPS has started monitoring with <Policy name> policy and Fabric Watch is disabled from monitoring.`

Message Type: LOG | AUDIT

Class: MAPS

Severity:INFO

Probable Cause: Indicates that MAPS has started monitoring the system and therefore Fabric Watch monitoring has been disabled.

Recommended Action: Make sure the configuration change is expected.

MAPS-1202

Message: `MAPS Disabled.`

Message Type: LOG | AUDIT

Class: MAPS

Severity:INFO

Probable Cause: Indicates that MAPS has been disabled. MAPS will continue to monitor the system until reboot .

Recommended Action: Make sure the configuration change is expected. To activate Fabric Watch monitoring and disable MAPS, reboot or fail over the system.

MAPS-1203

Message: `dashboard <data type> data has been cleared.`

Message Type: LOG | AUDIT

Class: MAPS

Severity:WARNING

Probable Cause: Indicates that the dashboard has been cleared.

Recommended Action: No action is required.

MCST Messages

MCST-1001

Message:`Socket Error: <op> (<reason>) for socket <sockname> the error code<errorname>.`

Message Type: DCE

Severity: ERROR

Probable Cause: Indicates that an error has occurred in the Linux socket.

Recommended Action: Reload or power cycle the switch.

MCST-1002

Message: `Socket Error: <op> sock name <sock> Error <error> type <type> seq <seq> pid <pid>.`

Message Type: DCE

Severity: ERROR

Probable Cause: Indicates that the specified error has occurred while processing the hardware abstraction layer (HAL) message.

Recommended Action: Reload or power cycle the switch.

MCST-1003

Message: `Learning error: <op> (<reason>) - VLAN <vid> MAC/group <address>.`

Message Type: DCE

Severity: ERROR

Probable Cause: Indicates that the multicast subsystem (mcast_ss) has encountered an error while learning the media access control (MAC) addresses.

Recommended Action: Reload or power cycle the switch.

MCST-1004

Message: `NSM error: <op> (<reason>) for VLAN <vid> port <port>.`

Message Type: DCE

Severity: ERROR

Probable Cause: Indicates that the multicast subsystem (mcast_ss) has encountered an error during a network service module (NSM) event.

Recommended Action: Reload or power cycle the switch.

MCST-1005

Message: `Message error: Invalid message type <type> expecting <value1> or <value2> or <value3>.`

Message Type: DCE

Severity: ERROR

Probable Cause: Indicates that the type of the message received from the driver is invalid

Recommended Action: Reload or power cycle the switch.

MCST-1006

Message: `Message error: <op> (<reason>)Invalid message length <length> expecting <length1>.`

Message Type: DCE

Severity: ERROR

Probable Cause: Indicates that the length of the message received from the driver is invalid.

Recommended Action: Reload or power cycle the switch.

MCST-1007

Message: `Initialization error: <op> (<reason>).`

Message Type: DCE

Severity: ERROR

Probable Cause: Indicates that the multicast subsystem (mcast_ss) has encountered an error during initialization.

Recommended Action: Reload or power cycle the switch.

MCST-1008

Message: `HAL error: <op> (<reason>) - VLAN <vid> MAC/group <address>.`

Message Type: DCE

Severity: ERROR

Probable Cause: Indicates that the multicast subsystem (mcast_ss) has encountered the hardware abstraction layer (HAL) errors.

Recommended Action: Reload or power cycle the switch.

MCST-1009

Message: `L2SS error: <op> (<reason>) VLAN <vid> MAC <mac address>.`

Message Type: DCE

Severity: ERROR

Probable Cause: Indicates that the multicast subsystem (mcast_ss) has encountered the Layer 2 subsystem (L2SS) related errors.

Recommended Action: Reload or power cycle the switch.

MCST-1010

Message: `Message Queue error: <op> (<reason>) TYPE <type>.`

Message Type: DCE

Severity: ERROR

Probable Cause: Indicates that the multicast subsystem (mcast_ss) has encountered the message queue errors.

Recommended Action: Reload or power cycle the switch.

MCST-1011

Message: `IDB error: <op> (<reason>) port index <port-index> not found for VLAN ID <vlan-id>.`

Message Type: DCE

Severity: ERROR

Probable Cause: Indicates that the specified port index is invalid.

Recommended Action: If there is an impact on the data path, reload or power cycle the switch. Refer to the Network OS Administrator's Guide for instructions to verify the data path.

MCST-1012

Message: `IDB error: <op> (<reason>) VLAN ID <vid> not found.`

Message Type: DCE

Severity: ERROR

Probable Cause: Indicates that the specified VLAN ID (VID) is invalid.

Recommended Action: If there is an impact on the data path, reload or power cycle the switch. Refer to the Network OS Administrator's Guide for instructions to verify the data path.

MCST-1013

Message: `Snooping DB error: <op> (<reason>) Group not found - VLAN <vid> group <group address>.`

Message Type: DCE

Severity: ERROR

Probable Cause: Indicates that the group address lookup for the specified VLAN has failed.

Recommended Action: Reload or power cycle the switch.

MCST-1014

Message: `Snooping DB error: <op> (<reason>) MAC not found - VLAN <vid> MAC-addr <MAC address>.`

Message Type: DCE

Severity: ERROR

Probable Cause: Indicates that the media access control (MAC) address lookup for the specified VLAN has failed.

Recommended Action: Reload or power cycle the switch.

MCST-1015

Message: `HSL error: <op> (<reason>) failed for message <message> VLAN <vid> MAC <MAC address> mgid <mgid> CPU <cpu>.`

Message Type: DCE

Severity: ERROR

Probable Cause: Indicates that the specified hardware subsystem layer (HSL) related operation has failed.

Recommended Action: Reload or power cycle the switch.

MCST-1016

Message: `Message error: <op> (<reason>) <length> (<length1>).`

Message Type: DCE

Severity: ERROR

Probable Cause: Indicates that the length of the message received from the driver is invalid.

Recommended Action: Reload or power cycle the switch.

MCST-1017

Message: `Learning error: <op> (<reason>) Invalid number <port> for ifindex <ifindex>.`

Message Type: DCE

Severity: ERROR

Probable Cause: Indicates that the multicast subsystem (mcast_ss) has encountered an error while learning the media access control (MAC) addresses.

Recommended Action: Reload or power cycle the switch.

MCST-1018

Message: `Memory Alloc Error: <op> (<reason>) type <memtype>/<memsize>.`

Message Type: DCE

Severity: ERROR

Probable Cause: Indicates that the multicast subsystem (mcast_ss) has encountered an error during the memory allocation.

Recommended Action: Reload or power cycle the switch.

MCST-1019

Message: `Ptree Error: <op> (<reason>) VLAN <vid> MAC/group <address>.`

Message Type: DCE

Severity: ERROR

Probable Cause: Indicates that the multicast subsystem (mcast_ss) has encountered an error during the Ptree operation.

Recommended Action: Reload or power cycle the switch.

MCST-1020

Message: `List Error: <op> (<reason>) VLAN <vid> MAC <mac address> group <group address>.`

Message Type: DCE

Severity: ERROR

Probable Cause: Indicates that the multicast subsystem (mcast_ss) has encountered an error during the List operation.

Recommended Action: Reload or power cycle the switch.

MM Messages

MM-1001

Message:`VPD block 0 CRC is bad.`

Message Type: LOG

Severity: WARNING

Probable Cause:

Indicates that CRC in the VPD block 0 is bad. This could indicate corruption or tampering.

This message occurs only on the Extreme VDX 2740 switch.

Recommended Action: Execute the **`copy support`** command and contact your switch service provider.

MPTH Messages

MPTH-1001

Message:`Null parent, lsId = <number>.`

Message Type: LOG | FFDC

Severity: ERROR

Probable Cause: Indicates that a null parent was reported. The minimum cost path (MPATH) uses a tree structure in which the parent is used to connect to the root of the tree.

Recommended Action: No action is required.

MPTH-1002

Message: `Null lsrP, lsId = <ls ID number>.`

Message Type: LOG | FFDC

Severity: ERROR

Probable Cause: Indicates that the link state record (LSR) is null.

Recommended Action: No action is required.

MPTH-1003

Message: `No minimum cost path in candidate list.`

Message Type: LOG

Severity: WARNING

Probable Cause: Indicates the fabric shortest path first (FSPF) module has determined that there is no minimum cost path (MPATH) available in the candidate list.

Recommended Action: No action is required.

MSTP Messages

MSTP-1001

Message:`Unable to allocate memory.`

Message Type: DCE

Severity: ERROR

Probable Cause: Indicates that the system has failed to allocate memory.

Recommended Action: Check the memory usage on the switch using the **`show process memory`** command.

Reload or power cycle the switch.

MSTP-1002

Message: `Error start DCM client.`

Message Type: DCE

Severity: ERROR

Probable Cause: Indicates that the system has failed to initialize.

Recommended Action: Reload or power cycle the switch.

MSTP-1003

Message: `PDU[RECV]: receive failed.`

Message Type: DCE

Severity: ERROR

Probable Cause: Indicates a connection, transfer, or receiving error in the socket.

Recommended Action: If this is a modular switch, execute the command. If the problem persists or if this is a compact switch, download a new firmware version using the **`firmware download`** command.

MSTP-1004

Message: `Received BPDU on PortFast enable port. Shutting down Interface <message>`

Message Type: DCE

Severity: ERROR

Probable Cause: Indicates that a port on which PortFast is enabled has received a bridge protocol data unit (BPDU). The port has been disabled.

Recommended Action: Disable the PortFast feature on the port using one of the following commands:

• For Rapid Spanning Tree Protocol (RSTP), execute the **`no spanning-tree edgeport`** command.

• For Spanning Tree Protocol (STP), execute the **`no spanning-tree portfast`** command.

After disabling the PortFast feature, execute the **`no shutdown`** command to re-enable the port.

MSTP-2001

Message: `[MSTP-2001], 4653, DCE, INFO, SLX, Spanning Tree mode changed to (Rapid-PVST).`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that the Multiple Spanning Tree Protocol (MSTP) bridge mode has changed.

Recommended Action: No action required.

MSTP-2002

Message: `<Bridge mode information>. My Bridge ID: <Bridge ID> Old Root: <Old Root ID> New Root: <New Root ID>.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that the Multiple Spanning Tree Protocol (MSTP) bridge or bridge instance root has been changed.

Recommended Action: No action required.

MSTP-2003

Message: `MSTP instance <instance> is created.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that the specified Multiple Spanning Tree Protocol (MSTP) instance has been created.

Recommended Action: No action required.

MSTP-2004

Message: `MSTP instance <instance> is deleted.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that the specified Multiple Spanning Tree Protocol (MSTP) instance has been deleted.

Recommended Action: No action required.

MSTP-2005

Message: `VLAN <vlan_ids> is <action> on MSTP instance <instance>.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that the specified Multiple Spanning Tree Protocol (MSTP) instance has been modified.

Recommended Action: No action required.

MSTP-2006

Message: `MSTP instance <instance> bridge priority is changed from <priority_old> to <priority_new>.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that the specified Multiple Spanning Tree Protocol (MSTP) instance priority has been modified.

Recommended Action: No action required.

MSTP-2007

Message: `<Bridge mode information>: <vlan/instance and port> - STP state <state>`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that the STP port state has been changed.

Recommended Action: No action required.

MSTP-3003

Message: `Could not restore spanning tree state for interface <ifName>. Maximum port count reached.`

Message Type: DCE

Severity:ERROR

Probable Cause: Indicates that the system ran out of port ID space, probably due to stale entries in the system. The maximum port count for STP and PVST is 1 through 255, and for RSTP, MSTP, and RPVST the maximum port count is 1 through 4095.

Recommended Action: Shut down spanning tree on interfaces that are no longer required using the **`spanning-tree shutdown`** command and try the operation again.

NSM Messages

NSM-1001

Message:`interface <InterfaceName> is online.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that the specified interface has come online after the protocol dependencies are resolved.

Recommended Action: No action is required.

NSM-1002

Message: `interface <InterfaceName> is protocol down.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that the specified interface has gone offline because one of the protocol dependency is unresolved.

Recommended Action: Check for the reason codes using the show interface command and resolve the protocol dependencies.

NSM-1003

Message: `interface <InterfaceName> is link down.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that the specified interface has gone offline because the link was down.

Recommended Action: Check whether the connectivity is proper and the remote link is up.

NSM-1004

Message: `<InterfaceName> is created.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that the specified logical interface has been created

Recommended Action: No action is required.

NSM-1007

Message: `Chassis is <status>.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that the chassis has been enabled or disabled.

Recommended Action: No action is required.

NSM-1009

Message: `<InterfaceName> is deleted.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that the specified logical interface has been deleted.

Recommended Action: No action is required.

NSM-1010

Message: `InterfaceMode changed from <Mode_old> to <Mode_new> for interface <InterfaceName>.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that the interface mode has been changed.

Recommended Action: No action is required.

NSM-1011

Message: `OperationalEndpointMode changed from <Mode_old> to <Mode_new> for interface <InterfaceName>.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that the interface operational endpoint mode has been changed.

Recommended Action: No action is required.

NSM-1012

Message: `VLAN classifier group <group_id> is created.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that the specified VLAN classifier group has been created.

Recommended Action: No action is required.

NSM-1013

Message: `VLAN classifier group <group_id> is deleted.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that the specified VLAN classifier group has been deleted.

Recommended Action: No action is required.

NSM-1014

Message: `VLAN classifier rule <rule_id> is created.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that the specified VLAN classifier rule has been created.

Recommended Action: No action is required.

NSM-1015

Message: `VLAN classifier rule <rule_id> is deleted.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that the specified VLAN classifier rule has been deleted.

Recommended Action: No action is required.

NSM-1016

Message: `VLAN classifier rule <rule_id> is <action> on VLAN classifier group <group_id>.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that the specified VLAN classifier group has been modified.

Recommended Action: No action is required.

NSM-1017

Message: `Interface <InterfaceName> is <action> on interface <Logical_InterfaceName>.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that the specified logical interface member list has been changed.

Recommended Action: No action is required.

NSM-1018

Message: `<count> VLANs <except> will be allowed on interface <Logical_InterfaceName>.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that the VLAN membership has been changed for the specified interface.

Recommended Action: No action is required.

NSM-1019

Message: `Interface <InterfaceName> is administratively up.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that the interface administrative status has changed to up.

Recommended Action: No action is required.

NSM-1020

Message: `Interface <InterfaceName> is administratively down.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that the interface administrative status has changed to down.

Recommended Action: No action is required.

NSM-1021

Message: `Interface IP overlap with management IP <ipAddr> ifname:<ifname>.`

Message Type: DCE

Severity: ERROR

Probable Cause: Indicates that the IP address configured on the interface overlaps with the management IP address.

Recommended Action: Change the interface IP address using the **`ip address`** command.

NSM-1022

Message: `FCoE configuration has been <Option> on interface <InterfaceName>.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that the Fibre Channel over Ethernet (FCoE) configuration has been enabled or disabled on the specified interface.

Recommended Action: No action is required.

NSM-1026

Message: `<SFPType> transceiver for interface <InterfaceName> is inserted.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that a (SFP/CFP2) transceiver has been inserted in the specified interface.

Recommended Action: No action is required.

NSM-1027

Message: `<SFPType> transceiver for interface <InterfaceName> is removed.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that a transceiver (SFP or CFP2) has been removed from the specified interface.

Recommended Action: No action is required.

NSM-1028

Message: `Incompatible SFP transceiver for interface <InterfaceName> is detected.`

Message Type: DCE

Severity: ERROR

Probable Cause: Indicates that an incompatible small form-factor pluggable (SFP) transceiver for the interface has been inserted.

Recommended Action: Disable the interface using the **shutdown** command and insert an SFP transceiver that is supported on the interface. After the SFP transceiver is inserted, re-enable the interface using the **no shutdown** command.

NSM-1029

Message: `Failed to read SFP transceiver for interface <InterfaceName>.`

Message Type: DCE

Severity: ERROR

Probable Cause: Indicates failure to read the small form-factor pluggable (SFP) transceiver for the specified interface.

Recommended Action: Disable the interface using the **shutdown** command and re-insert the SFP transceiver. After the SFP transceiver is inserted, re-enable the interface using the **no shutdown** command. If the problem persists, contact your switch service provider.

NSM-1030

Message: `Interface <InterfaceName> is administratively down due to speed mismatch in port-channel.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that the specified interface has gone down due to mismatching speed in the port-channel.

Recommended Action: Set the correct speed for the interface using the speed command.

NSM-1031

Message: `Session <SessionNumber> is created.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that the specified session has been created.

Recommended Action: No action is required.

NSM-1032

Message: `Session <SessionNumber> is deleted.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that the specified session has been deleted.

Recommended Action: No action is required.

NSM-1033

Message: `Session <SessionNumber> configuration is deleted.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that the specified session configuration has been deleted.

Recommended Action: No action is required.

NSM-1034

Message: `Session <SessionNumber> configuration is added.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that the specified session configuration has been added.

Recommended Action: No action is required.

NSM-1035

Message: `Description for Session <SessionNumber> is added.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that the session description has been added.

Recommended Action: No action is required.

NSM-1036

Message: `Description for Session <SessionNumber> is deleted.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that the session description has been deleted.

Recommended Action: No action is required.

NSM-1037

Message: `Interface <InterfaceName> is administratively down due to <LinkSpeed> link configured on Extreme Trunk.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that the specified interface has gone down because a 1 Gbps link has been configured on the Extreme trunk.

Recommended Action: Remove the 1 Gbps link from the Extreme trunk or change the 1 Gbps small form-factor pluggable (SFP) transceiver.

NSM-1038

Message: `Private VLAN mode changed from <Mode_old> to <Mode_new> for interface <InterfaceName>.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that the interface private VLAN mode has been changed.

Recommended Action: No action is required.

NSM-1039

Message: `Unsupported Extreme-branded SFP transceiver for interface <InterfaceName> is detected.`

Message Type: DCE

Severity: ERROR

Probable Cause: Indicates that an unsupported Extreme-branded small form-factor pluggable (SFP) transceiver has been inserted in the specified interface.

Recommended Action: Use a Extreme-branded SFP transceiver for the interface because the digital diagnostics will not be supported.

NSM-1040

Message: `Interface <InterfaceName> is unprovisioned.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that the specified logical interface has been unprovisioned.

Recommended Action: No action is required.

NSM-1041

Message: `interface <InterfaceName> is provisioned.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that the specified logical interface has been provisioned.

Recommended Action: No action is required.

NSM-1042

Message: `Unqualified SFP transceiver for interface <InterfaceName> is detected.`

Message Type: DCE

Severity:WARNING

Probable Cause: Indicates that an unqualified Extreme-branded small form-factor pluggable (SFP) transceiver has been inserted in the specified interface.

Recommended Action: Use a qualified Extreme-branded SFP transceiver for the interface because the digital diagnostics will not be supported.

NSM-1043

Message: `Unsupported SFP transceiver for interface <InterfaceName> is detected.`

Message Type: DCE

Severity: ERROR

Probable Cause: Indicates that an unsupported small form-factor pluggable (SFP) transceiver has been inserted in the specified interface.

Recommended Action: Use a qualified Extreme-branded SFP transceiver for the interface because the digital diagnostics will not be supported.

NSM-1044

Message: `interface <InterfaceName> is disabled by port link dampening.`

Message Type: DCE

Severity:INFO

Probable Cause: Indicates that the interface disabled due to port link dampening.

Recommended Action: No action is required.

NSM-1045

Message: `interface <InterfaceName> is enabled by port link dampening.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that the interface enabled due to port link dampening.

Recommended Action: No action is required.

NSM-1046

Message: `Topology group <TopoGrpId> master VLAN replaced from <OldmasterVlan> to <NewmasterVlan>.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that the master VLAN for the topology group has been replaced.

Recommended Action: No action is required.

NSM-1047

Message: `<VlanBd> <VlanBdId> configured as <MasterMember> of Topology group <TopoGrpId>.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates the VLAN/BD is configured as master/member for the topology group.

Recommended Action: No action is required.

NSM-1048

Message: `<VlanBd> <VlanBdId> removed from Topology group <TopoGrpId>.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates the master/member VLAN/BD removed from the topology group.

Recommended Action: No action is required.

NSM-1049

Message: `Topology group <TopoGrpId> deleted.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates topology group is deleted.

Recommended Action: No action is required.

NSM-1050

Message: `Message type <MessageType> length <MessageSize> from <ClientName> is too large.`

Message Type: DCE

Severity: ERROR

Probable Cause: Indicates that a message from the NSM client could not be processed because of its size.

Recommended Action: Increase size of NSM daemon buffer.

NSM-1051

Message: `<InterfaceName> interface is deleted.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that the specified physical/insight interface has been deleted.

Recommended Action: No action is required.

NSM-1052

Message: `IP unnumbered intf <InterfaceName> vrf must be same as donor inttf <InterfaceName> .`

Message Type: DCE

Severity: ERROR

Probable Cause: Indicates that ip unnumbered interface vrf is not same as donor interface vrf .

Recommended Action: Both unnumbered interface and donor interface vrf should be same.

NSM-1053

Message: `interface <InterfaceName> TAG Type Changed to 0x<tpid>.`

Message Type: DCE

Severity: ERROR, INFO. The severity will depend on the TAG Type ID, *tpid*.

Probable Cause: Indicates that interface TAG Type is being configured.

Recommended Action: No action is required.

NSM-1062

Message: `fec mode <RS-FEC | FC-FEC | Auto-Negotiation | Disabled>`

Message Type: DCE

Severity: ERROR

Probable Cause: This message is generated for all unsupported FEC modes on 100G optics(Passive DAC/SR4/LR4) , 40G and 10G from NSM module.

Recommended Action: Confirm the supported FEC modes for the optic in question with the Release Notes. Verify that the optic is configured for the appropriate FEC mode. If you attempt to configure any mode other than a supported mode for that optic, then an Error Message will be generated.

NSM-1063

Message: `Activating Maintenance Mode due to hardware failure detected on ICL.`

Message Type: DCE

Severity: WARNING

Probable Cause: Indicates that Maintenance Mode has been enabled.

Recommended Action: Remove or replace the pluggable media and reboot the device to recover.

NSM-1064

Message: `Activating Maintenance Mode due to hardware failures affecting more than 50% of Cluster Client/Track ports.`

Message Type: DCE

Severity: WARNING

Probable Cause: Indicates that Maintenance Mode has been enabled

Recommended Action: Remove or replace the pluggable media and reboot the device to recover.

NSM-1700

Message: `Tunnel <TunnelName> creation failed.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that the tunnel creation was unsuccessful.

Recommended Action: Technical support is required.

NSM-1701

Message: `VNI mapping for VLAN <VLAN> was unsuccessful.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that system could not map VNI to the VLAN for a VxLAN tunnel.

Recommended Action: Technical support is required.

NSM-1702

Message: `Enabling flooding for <TunnelName> was unsuccessful.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that system could not enable flooding for the specific tunnel.

Recommended Action: Technical support is required.

NSM-1703

Message: `P2P BD <BDId> not extended Vxlan Tunnel <TunnelName>.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that system could not extend p2p BD on vxlan tunnel.

Recommended Action: P2P BD can not be extended over vxlan tunnel.

NSM-2000

Message: `Port-profile <ProfileName> activation succeeded.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that the profile activation was successful.

Recommended Action: No action is required.

NSM-2001

Message: `Port-profile <ProfileName> activation failed, reason <Reason>.`

Message Type: DCE

Severity: ERROR

Probable Cause: Indicates that the profile activation was unsuccessful.

Recommended Action: Check the configuration and port-profile status using the **`show port-profile status`** command. Execute the **`copy support`** command and contact your switch service provider.

NSM-2002

Message: `Port-profile <ProfileName> deactivation succeeded.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that the profile deactivation was successful.

Recommended Action: No action is required.

NSM-2003

Message: `Port-profile <ProfileName> deactivation failed, reason <Reason>.`

Message Type: DCE

Severity: ERROR

Probable Cause: Indicates that the profile deactivation was unsuccessful.

Recommended Action: Check the configuration and port-profile status using the **show port-profile status** command. Execute the **copy support** command and contact your switch service provider.

NSM-2004

Message: `Port-profile <ProfileName> application succeeded on <InterfaceName>.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that the profile application was successful.

Recommended Action: No action is required.

NSM-2005

Message: `Port-profile <ProfileName> application failed on <InterfaceName>, reason <Reason>, removing any applied configuration.`

Message Type: DCE

Severity:ERROR

Probable Cause: Indicates that the profile application on the specified interface was unsuccessful.

Recommended Action: Check the configuration and port-profile status using the **show port-profile status** command. Execute the **copy support** command and contact your switch service provider.

NSM-2006

Message: `Port-profile <ProfileName> removed successfully on <InterfaceName>.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that the specified port-profile has been removed successfully.

Recommended Action: No action is required.

NSM-2007

Message: `interface <InterfaceName> became port-profile-port.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that the port-profile configuration mode has been enabled on the specified interface using the **port-profile-port** command.

Recommended Action: No action is required.

NSM-2008

Message: `Interface <InterfaceName> became non-port-profile-port.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that the port-profile configuration mode has been disabled on the specified interface using the **no port-profile-port** command.

Recommended Action: No action is required.

NSM-2010

Message: `Interface <InterfaceName> could not become non-port-profile-port.`

Message Type: DCE

Severity: ERROR

Probable Cause: Indicates that the port-profile configuration mode could not be disabled on the specified interface using the no port-profile-port command.

Recommended Action: Check the configuration and port-profile status using the **show port-profile status** command. Execute the **copy support** command and contact your switch service provider.

NSM-2011

Message: `Port-profile <ProfileName> removal failed on <InterfaceName>.`

Message Type: DCE

Severity: ERROR

Probable Cause: Indicates that the specified port-profile could not be removed.

Recommended Action: Execute the **copy support** command and contact your switch service provider.

NSM-2012

Message: `MAC <ProfileMac> is associated to port-profile <ProfileName>.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates successful association of the Virtual Machine (VM) Media Access Control (MAC) address with the specified port-profile.

Recommended Action: No action is required.

NSM-2013

Message: `MAC <ProfileMac> is disassociated from port-profile <ProfileName>.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates successful disassociation of the Virtual Machine (VM) Media Access Control (MAC) address from the specified port-profile.

Recommended Action: No action is required.

NSM-2014

Message: `VLAN sub-profile for port-profile <ProfileName> is created.`

Message Type: DCE

Severity: INFO

Probable Cause: Cause Indicates that the VLAN sub-profile has been created successfully.

Recommended Action: No action is required.

NSM-2015

Message: `Access VLAN <VlanId> is configured for port-profile <ProfileName>.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that the untagged VLAN has been configured for the specified port-profile.

Recommended Action: No action is required.

NSM-2016

Message: `Access VLAN is deleted from port-profile <ProfileName>.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that the untagged VLAN has been removed from the specified port-profile.

Recommended Action: No action is required.

NSM-2017

Message: `Port-profile <ProfileName> is configured for switching properties.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that the switching properties have been configured on the specified port-profile using the **`switchport`** command.

Recommended Action: No action is required.

NSM-2018

Message: `Switching properties are removed for port-profile <ProfileName>.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that the switching properties have been removed from the specified port-profile using the **`no switchport`** command.

Recommended Action: No action is required.

NSM-2019

Message: `The <ModeName> mode is configured for port-profile <ProfileName>.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that the specified mode has been configured for the port-profile using the **`switchport mode`** command.

Recommended Action: No action is required.

NSM-2020

Message: `The <ModeName> mode is de-configured for port-profile <ProfileName>.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that the specified mode has been removed for the port-profile using the **`switchport mode`** command.

Recommended Action: No action is required.

NSM-2021

Message: `The tagged VLANs <TaggedVlanStr> are configured for port-profile <ProfileName>.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that the specified tagged VLANs are configured in the VLAN sub-profile.

Recommended Action: No action is required.

NSM-2022

Message: `The tagged VLANs <TaggedVlanStr> are removed for port-profile <ProfileName>.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that the specified tagged VLANs have been removed from the VLAN sub-profile.

Recommended Action: No action is required.

NSM-2023

Message: `The tagged VLANs except <TaggedVlanStr> are configured for port-profile <ProfileName>.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that except the specified tagged VLANs, all other tagged VLANs are configured in the VLAN sub-profile.

Recommended Action: No action is required.

NSM-2024

Message: `All VLANs are configured as tagged VLANs for port-profile <ProfileName>.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that all the available tagged VLANs are configured in the specified VLAN sub-profile.

Recommended Action: No action is required.

NSM-2025

Message: `All tagged VLANs are removed for port-profile <ProfileName>.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that all the available tagged VLANs have been from the specified VLAN sub-profile.

Recommended Action: No action is required.

NSM-2026

Message: `Native VLAN <VlanId> is configured to port-profile <ProfileName>.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that the native VLAN has been configured for the specified port-profile.

Recommended Action: No action is required.

NSM-2027

Message: `Native VLAN is deleted from port-profile <ProfileName>.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that the native VLAN has been removed from the specified port-profile.

Recommended Action: No action is required.

NSM-2028

Message: `FCoE sub-profile for port-profile <ProfileName> is created.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that the Fibre Channel over Ethernet (FCoE) sub-profile has been created for the specified port-profile.

Recommended Action: No action is required.

NSM-2029

Message: `FCoE port is configured successfully for port-profile <ProfileName>.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that the Fibre Channel over Ethernet (FCoE) port has been configured for the specified port-profile.

Recommended Action: No action is required.

NSM-2030

Message: `FCoE port is removed successfully for port-profile <ProfileName>.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that the Fibre Channel over Ethernet (FCoE) port has been removed from the specified port-profile.

Recommended Action: No action is required.

NSM-2031

Message: `Port-profile <ProfileName> is created.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that the specified port-profile has been created successfully.

Recommended Action: No action is required.

NSM-2032

Message: `Port-profile <ProfileName> is removed.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that the specified port-profile has been removed successfully.

Recommended Action: No action is required.

NSM-2033

Message: `VLAN sub-profile for port-profile <ProfileName> is deleted.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that the VLAN sub-profile has been deleted successfully.

Recommended Action: No action is required.

NSM-2034

Message: `FCoE sub-profile for port-profile <ProfileName> is deleted.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that the Fibre Channel over Ethernet (FCoE) sub-profile has been deleted successfully.

Recommended Action: No action is required.

NSM-2035

Message: `Non-profiled-macs on profiled ports will be <allowflag>.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that the non-profiled media access control (MAC) entries on the profiled port will be allowed or dropped.

Recommended Action: No action is required.

NSM-2036

Message: `Association of MAC address: <MAC> failed. Reason : <Reason>.`

Message Type: DCE

Severity: ERROR

Probable Cause: Indicates that an error occurred during port-profile to media access control (MAC) association.

Recommended Action: Check the configuration and port-profile status using the **`show port-profile status`** command. Execute the **`copy support`** command and contact your switch service provider.

NSM-2037

Message: `De-Association of MAC address: <MAC> failed. For Port-profile : <Reason>.`

Message Type: DCE

Severity: ERROR

Probable Cause: Indicates that an error occurred during port-profile to media access control (MAC) de-association.

Recommended Action: Check the configuration and port-profile status using the **`show port-profile status`** command. Execute the **`copy support`** command and contact your switch service provider.

NSM-2038

Message: `Bulk MAC association is Success for port-profile: <ProfileName>.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that all media access control (MAC) entries are successfully associated with the specified port-profile.

Recommended Action: No action is required.

NSM-2039

Message: `Bulk MAC de-association is Success for port-profile: <ProfileName>.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that all media access control (MAC) entries are successfully de-associated with the specified port-profile.

Recommended Action: No action is required.

NSM-2040

Message: `Ctag <Ctag> is associated with Virtual Fabric <virtual fabric> for port-profile: <ProfileName>.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates successful association of the c-tag with virtual fabric on the specified port-profile.

Recommended Action: No action is required.

NSM-2041

Message: `MAC <Mac> is associated with Virtual Fabric <virtual fabric> for port-profile: <ProfileName>.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates successful association of Media Access Control (MAC) with virtual fabric on the specified port-profile.

Recommended Action: No action is required.

NSM-2042

Message: `Ctag <Ctag> is deassociated with Virtual Fabric <virtual fabric> for port-profile: <ProfileName>.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates successful disassociation of the c-tag with virtual fabric on the specified port-profile.

Recommended Action: No action is required.

NSM-2043

Message: `MAC <Mac> is deassociated with Virtual Fabric <virtual fabric> for port-profile: <ProfileName>.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates successful disassociation of Media Access Control (MAC) with virtual fabric on the specified port-profile.

Recommended Action: No action is required.

NSM-2044

Message: `Domain: <DomainName> creation successful.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that the specified domain is created.

Recommended Action: No action is required.

NSM-2045

Message: `Domain deletion <DomainName> successful.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that the specified domain is deleted.

Recommended Action: No action is required.

NSM-2046

Message: `Profile: <ProfileName> addition to domain <DomainName> successful.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that the port-profile is added to the specified domain.

Recommended Action: No action is required.

NSM-2047

Message: `Profile <ProfileName> deletion from domain <DomainName> successful.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that the port-profile is deleted from the specified domain.

Recommended Action: No action is required.

NSM-2048

Message: `VLAN classifier mac-group <group_id> is created.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that the specified VLAN classifier MAC group has been created.

Recommended Action: No action is required.

NSM-2049

Message: `DAD failed for IPv6 address <IPv6 Address> on interface <Interface name>.`

Message Type: DCE

Severity: ERROR

Probable Cause: Indicates that the DHCP Auto Deployment (DAD) process failed for the specified IPv6 address.

Recommended Action: Delete the rejected IPv6 address and configure a corrected IPv6 address.

NSM-2050

Message: `Netdevice creation failed for interface <Interface name>.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that the system could not create a netdevice for the specified interface.

Recommended Action: No action is required.

NSM-2051

Message: `Port-profile <ProfileName> application failed on <InterfaceName>, for vlan <Vlan>, reason <Reason>`

Message Type: DCE

Severity: ERROR

Probable Cause: Indicates that the profile application on the specified interface was unsuccessful.

Recommended Action: Check the configuration and port-profile status using the **`show port-profile status`** command. Execute the **`copy support`** command and contact your switch service provider.

NSM-2052

Message: `VLAN <VLAN ID> is <action> on interface <InterfaceName> for Client: <Client MAC> by Dot1x.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that the Radius Dynamic VLAN is changed by dot1x.

Recommended Action: No action is required.

NSM-2053

Message: `Unnumbered Intf's peer ipv4 addr <IPv4 Address> is overlapped and can't be added on interface <InterfaceName>,reason <reason>.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that invalid peer address is received.

Recommended Action: change unnumbered peer ipv4 address.

NSM-2071

Message: `Chassis beaconing is enabled`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that chassis beaconing is enabled

Recommended Action: No action is required.

NSM-2072

Message: `Chassis beaconing is disabled`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that chassis beaconing is disabled

Recommended Action: No action is required.

NSM-2073

Message: `Interface beaconing on <InterfaceName> is enabled`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that interface beaconing is enabled.

Recommended Action: No action is required.

NSM-2074

Message: `Interface beaconing on <InterfaceName> is disabled`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that interface beaconing is disabled.

Recommended Action: No action is required.

NSM-2075

Message: `Interface loopback on <Interface Name> is enabled`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that interface loopback is enabled.

Recommended Action: No action is required.

NSM-2076

Message: `Interface loopback on <Interface Name> is disabled`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that interface loopback is disabled.

Recommended Action: No action is required.

NSM-3001

Message: `BD ID <BD ID> of type <BD Type> is Operationally UP.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that the BD is operationally UP.

Recommended Action: No action is required.

NSM-3002

Message: `BD ID <BD ID> of type <BD Type> is Operationally DOWN.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that the BD is operationally DOWN.

Recommended Action: No action is required.

NSM-3003

Message: `First pw lif in BD <BD ID> is Operationally UP.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that the first pw lif in BD is operationally UP.

Recommended Action: No action is required.

NSM-3004

Message: `Last pw lif in BD <BD ID> is Operationally down.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that the last pw lif in BD is operationally down.

Recommended Action: No action is required.

NSM-3005

Message: `Bridge Domain <BD ID> is created.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that the BD is created.

Recommended Action: No action is required.

NSM-3006

Message: `Bridge Domain <BD ID> is deleted.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that the BD is deleted.

Recommended Action: No action is required.

NSM-3007

Message: `Logical interface(LIF) resource has reached user configured high threshold limit.`

Message Type: DCE

Severity: INFO

Probable Cause: The LIF table has reached the user configured high threshold limit.

Recommended Action: Reduce the number of LIF entries in the table.

NSM-3008

Message: `Configuration of AC LIFs has reached the system max allowed AC LIFs.`

Message Type: DCE

Severity: INFO

Probable Cause: The number of user configured AC LIFs has reached the system's maximum allowed AC LIFs.

Recommended Action: Reduce the number of user configured AC LIFs.

NSM-4000

Message: `<pkt-encap-processing feature> is <enable> on interface <interface>.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates the config received from dcmd.

Recommended Action: No action is required.

OFMA Messages

OFMA-1001

Message:`Openflow Agent Ready Meta: <meta>`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that a new controller is connected.

Recommended Action: No action is required.

OFD Messages

OFD-1001

Message:`Controller Name: <message> Status: <>`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that an OpenFlow controller has been connected/connecting.

Recommended Action: No action is required.

OFD-1002

Message: `Controller Name: <message> Status: <> Reason: <>`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that an OpenFlow controller has been disconnected/ disconnecting.

Recommended Action: No action is required.

OFD-1003

Message: `Controller Name: <message> role changed to: <>`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that an OpenFlow controller has changed Role

Recommended Action: No action is required.

OFD-2000

Message: `Warning Message:%s`

Message Type: LOG

Severity: WARNING

Probable Cause: Warning message in openflow (DEPRECATED)

Recommended Action: Please check the warning

OFD-3000

Message: `Controller Name: <message>, xid <> (0x<>), Command: <>, Reason: <>`

Message Type: LOG

Severity: ERROR

Probable Cause: Indicates an error with openflow protocol

Recommended Action: Re-check the openflow protocol message sent

OFD-3001

Message: `Controller Name: <message>, xid <> (0x<>), Command: <>, Reason: <>`

Message Type: LOG

Severity: ERROR

Probable Cause: Indicates that the flow/group/meter operation failed.

Recommended Action: Re-check the flow/group/meter mod message. This could be either due to protocol error or hardware limitation.

ONMD Messages

ONMD-1000

Message: `LLDP is enabled.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that the Link Layer Discovery Protocol (LLDP) is enabled globally.

Recommended Action: No action is required.

ONMD-1001

Message:`LLDP is disabled.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that the Link Layer Discovery Protocol (LLDP) is disabled globally.

Recommended Action: No action is required.

ONMD-1002

Message: `LLDP global configuration is changed.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that the Link Layer Discovery Protocol (LLDP) global configuration has been changed.

Recommended Action: No action is required.

ONMD-1003

Message: `LLDP is enabled on interface <InterfaceName>.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that the Link Layer Discovery Protocol (LLDP) is enabled on the specified interface.

Recommended Action: No action is required.

ONMD-1004

Message: `LLDP is disabled on interface <InterfaceName>.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that the Link Layer Discovery Protocol (LLDP) is disabled on the specified interface.

Recommended Action: No action is required.

ONMD-1005

Message: `Feature Mismatch: <Feature>, will re-negotiate.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that the content of the specified feature does not match with the link partner.

Recommended Action: Change the feature setting at both ends of the link to match.

ONMD-1006

Message: `Timed out waiting for LLDP PDUs on <InterfaceName> from MAC address <MacAdress>.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that the Link Layer Discovery Protocol (LLDP) PDUs are not received from the neighbor for the configured period of time.

Recommended Action: No action is required.

ONMD-1007

Message: `Received First LLDP PDU on <InterfaceName> from MAC address <MacAdress> after LLDP RX enabled or timeout.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that the Link Layer Discovery Protocol (LLDP) PDUs are being received from the neighbor.

Recommended Action: No action is required.

ONMD-1008

Message: `Received shutdown LLDP PDUs with TTL=0 on <InterfaceName> from MAC address <MacAdress>.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that shutown Link Layer Discovery Protocol (LLDP) PDUs are received.

Recommended Action: No action is required.

OSPF Messages

OSPF-1001

Message: `Configuration Error RID %s. Interface Address %s. Pkt Srcaddress %s. Error Type %s Pkt Type %s.`

Message Type: DCE

Severity: ERROR

Probable Cause: Indicates a configuration error.

Recommended Action: Make sure to input or pass the right parameter through CLI or other daemon.

OSPF-1002

Message: `%s:%u`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates an open shortest path first (OSPF) interface state change or external link-state database (LSDB) overflow notification.

Recommended Action: No action required.

OSPF-1003

Message: `%s. Error Type %s. RID %s. Intf Addr %s. Pkt Src Addr %s. Pkt Type %s.`

Message Type: DCE

Severity: ERROR

Probable Cause: Indicates that the length, format, or content of the received packet is incorrect.

Recommended Action: Check configuration at the local or remote node.

OSPF-1004

Message: `Neighbor state changed. RID %s. Intf %s. Nbr Addr %s. Nbr RID %s. State %s.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates an open shortest path first (OSPF) neighbor state change to full adjacency.

Recommended Action: No action required.

OSPF-1005

Message: `Neighbor state changed. RID %s. Intf %s. Nbr Addr %s. Nbr RID %s. State %s. Reason %s`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates an open shortest path first (OSPF) neighbor state change to down or Init from FULL state.

Recommended Action: No action required.

OSPF6 Messages

OSPF6-1001

Message:<Configuration Error RID %s>.

Message Type:DCE

Severity: ERROR

Probable Cause: Indicates a configuration error.

Recommended Action: Make sure to input or pass the right parameter through CLI or other daemon.

OSPF6-1002

Message: <Interface state change information/overflow notification>.

Message Type:DCE

Severity: INFO

Probable Cause: Indicates an open shortest path first version 3(OSPFv3) interface state change or external link-state database (LSDB) overflow notification.

Recommended Action: No action is required.

OSPF6-1003

Message: <Rx packet error>.

Message Type:DCE

Severity: ERROR

Probable Cause: Indicates that the length, format, or content of the received packet is incorrect.

Recommended Action: Check configuration at the local or remote node.

PCAP Messages

PCAP-1001

Message: Packet capture enabled on the <Port name> interface.

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that packet capture is enabled on the specified interface.

Recommended Action: No action is required.

PCAP-1002

Message: `Packet capture disabled on the <Port name> interface.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that packet capture is disabled on the specified interface.

Recommended Action: No action is required.

PCAP-1003

Message: `Packet capture disabled globally.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that packet capture is disabled globally on the switch.

Recommended Action: No action is required.

PCAP-1004

Message: `<filename> file is created. Location is flash://<filename>.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that the specified .pcap file has been created.

Recommended Action: No action is required.

PDM Messages

PDM-1001

Message:`Failed to parse the pdm config.`

Message Type: LOG

Severity: WARNING

Probable Cause: Indicates that the parity data manager (PDM) process could not parse the configuration file. This may be caused due to a missing configuration file during the installation.

Recommended Action: Execute the firmware download command to reinstall the firmware.

If the message persists, execute the copy support command and contact your switch service provider.

PDM-1003

Message: `pdm [-d] -S <service> -s <instance>.`

Message Type: LOG

Severity: WARNING

Probable Cause: Indicates that a syntax error occurred when trying to launch the parity data manager (PDM) process.

Recommended Action: Execute the firmware download command to reinstall the firmware.

If the message persists, execute the copy support command and contact your switch service provider.

PDM-1004

Message: `PDM memory shortage.`

Message Type: LOG

Severity: WARNING

Probable Cause: Indicates that the parity data manager (PDM) process ran out of memory.

Recommended Action: Restart or power cycle the switch.

If the message persists, execute the copy support command and contact your switch service provider.

PDM-1006

Message: `Too many files in sync.conf.`

Message Type: LOG

Severity: WARNING

Probable Cause: Indicates that the sync.conf configuration file contains too many entries.

Recommended Action: Execute the **`firmware download`** command to reinstall the firmware.

If the message persists, execute the **copy support** command and contact your switch service provider.

PDM-1007

Message: `File not created: <file name>. errno=<errno>.`

Message Type: LOG

Severity: WARNING

Probable Cause: Indicates that the parity data manager (PDM) process failed to create the specified file.

Recommended Action: Execute the **firmware download** command to reinstall the firmware.

If the message persists, execute the **copy support** command and contact your switch service provider.

PDM-1009

Message: `Cannot update Port Config Data.`

Message Type: LOG

Severity: WARNING

Probable Cause: Indicates that the parity data manager (PDM) system call for setting port configuration (setCfg) failed.

Recommended Action: Execute the **firmware download** command to reinstall the firmware.

If the message persists, execute the **copy support** command and contact your switch service provider.

PDM-1010

Message: `File open failed: <file name>, errno=<errno>.`

Message Type: LOG

Severity: WARNING

Probable Cause: Indicates that the parity data manager (PDM) process could not open the specified file.

Recommended Action: Execute the **firmware download** command to reinstall the firmware.

If the message persists, execute the **copy support** 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

Severity: WARNING

Probable Cause: Indicates that the parity data manager (PDM) process could not read data from the specified file.

Recommended Action: Execute the **`firmware download`** command to reinstall the firmware.

If the message persists, execute the **`copy support`** 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

Severity: WARNING

Probable Cause: Indicates that the parity data manager (PDM) process could not write data to the specified file.

Recommended Action: Execute the **`firmware download`** command to reinstall the firmware.

If the message persists, execute the **`copy support`** command and contact your switch service provider.

PDM-1013

Message: `File empty: <File Name>.`

Message Type: LOG

Severity: WARNING

Probable Cause: Indicates that the switch configuration file /etc/fabos/fabos.[0|1].conf is empty.

Recommended Action: Execute the **`firmware download`** command to reinstall the firmware.

If the message persists, execute the **`copy support`** command and contact your switch service provider.

PDM-1014

Message: `Access sysmod failed.`

Message Type: LOG

Severity: WARNING

Probable Cause: Indicates that a system call to sysMod failed.

Recommended Action: Execute the **`firmware download`** command to reinstall the firmware.

If the message persists, execute the **`copy support`** command and contact your switch service provider.

PDM-1017

Message: `System (<Error Code>): <Command>.`

Message Type: FFDC | LOG

Severity:CRITICAL

Probable Cause: Indicates that the specified system call failed.

Recommended Action: Execute the **`firmware download`** command to reinstall the firmware.

If the message persists, execute the **`copy support`** command and contact your switch service provider.

PDM-1019

Message: `File path or trigger is too long.`

Message Type: LOG

Severity: WARNING

Probable Cause: Indicates that a line in the pdm.conf file is too long.

Recommended Action: Execute the **`firmware download`** command to reinstall the firmware.

If the message persists, execute the **`copy support`** command and contact your switch service provider.

PDM-1021

Message: `Failed to download area port map.`

Message Type: LOG

Severity: WARNING

Probable Cause: Indicates that a system call failed.

Recommended Action: Execute the **`firmware download`** command to reinstall the firmware.

If the message persists, execute the **`copy support`** command and contact your switch service provider.

PHP Messages

PHP-1001

Message:`<INFO %s>.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates a user-defined informative message.

Recommended Action: No action is required.

PHP-1002

Message: `<WARNING %s>.`

Message Type: LOG

Severity: WARNING

Probable Cause: Indicates a user-defined warning message.

Recommended Action: No action is required.

PHP-1003

Message: `<ERROR %s>.`

Message Type: LOG

Severity: ERROR

Probable Cause: Indicates a user-defined error message.

Recommended Action: No action is required.

PHP-1004

Message: `<CRITICAL %s>.`

Message Type: LOG

Severity: CRITICAL

Probable Cause: Indicates a user-defined critical message.

Recommended Action: No action is required.

PIM Messages

PIM-1001

Message:`<message> init failed.`

Message Type: LOG

Severity: ERROR

Probable Cause: Indicates that an internal failure occurred during sub-system initialization.

Recommended Action: Make sure the switch has enough memory to initialize the sub-system.

PIM-1002

Message: `<message> on port <port number>. PIM enable failed.`

Message Type: LOG

Severity: ERROR

Probable Cause: Indicates an issue while enabling PIM on interface.

Recommended Action: Verify port configuration and status.

PLAT Messages

PLAT-1000

Message:`<Function name> <Error string>.`

Message Type: FFDC | LOG

Severity: CRITICAL

Probable Cause: Indicates that nonrecoverable peripheral component interconnect (PCI) errors have been detected.

Recommended Action: The system will be faulted and may reload automatically.

If the system does not reload, execute the reload command.

Execute the copy support command and contact your switch service provider.

PLAT-1001

Message: `MM<Identifies which MM (1 or 2) is doing the reset> resetting other MM (double reset may occur).`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that the other management module is being reset. This message is typically generated by a management module that is in the process of becoming the active management module. Note that in certain circumstances a management module may experience a double reset and reload twice. A management module can recover automatically even if it has reloaded twice.

Recommended Action: No action is required.

PLAT-1002

Message: `MM<Identifies which MM (1 or 2) is generating the message>: <Warning message> hk_fence 0x<MM Housekeeping Fence register. Contents are platform-specific> mm_ha 0x<MM HA register. Contents are platform-specific> mm_status 0x<MM Status register. Contents are platform-specific>.`

Message Type: LOG

Severity: WARNING

Probable Cause: Indicates that one of the management modules cannot access the inter-integrated circuit (I2C) subsystem because of an error condition or being isolated from the I2C bus.

Recommended Action: Reload the management module if it does not reload automatically. Reseat the management module if reloading does not solve the problem. If the problem persists, replace the management module.

PLAT-1004

Message: `Turning off Fan <Fan Number> because of airflow direction mismatch.`

Message Type: LOG | FFDC

Severity: CRITICAL

Probable Cause: Indicates that the specified fan field-replaceable unit (FRU) has been turned off because it is incompatible with the system airflow direction policy.

Recommended Action: Replace the fan FRU. Refer to the Hardware Reference Manual of your switch for instructions to replace the fan FRU.

PLAT-1005

Message: `Unable to read EEPROM for Global airflow direction. Setting to default Port side intake.`

Message Type: LOG | FFDC

Severity: CRITICAL

Probable Cause: Indicates a failure to read the electrically erasable programmable read-only memory (EEPROM) to determine the airflow direction of the fans. Therefore, setting the airflow direction to be from the port side of the system.

Recommended Action: Execute the **`copy support`** command and contact your switch service provider.

PLAT-1006

Message: `Unable to read EEPROM for Global airflow direction. Shutting off Fans now.`

Message Type: LOG

Severity: CRITICAL

Probable Cause: Indicates a failure to read the electrically erasable programmable read-only memory (EEPROM) to determine the airflow direction of the fans. The fans will be shut down.

Recommended Action: Execute the **`copy support`** command and contact your switch service provider.

PLAT-1007

Message: `Turning off Fan <Fan Number> because of airflow direction <Global airflow direction>.`

Message Type: LOG

Severity: ERROR

Probable Cause: Indicates that the specified fan is turned off because of an incorrect airflow direction.

Recommended Action: Replace the fan field-replaceable units (FRUs) in such a manner that the air flows in the same direction, that is, towards the port side or away from the port side of the system. Refer to the Hardware Reference Manual of your switch for instructions to replace the fan FRU.

PLAT-1008

Message: `Unable to read EEPROM for Global airflow direction.`

Message Type: LOG

Severity: ERROR

Probable Cause: Indicates a failure to read the electrically erasable programmable read-only memory (EEPROM) and therefore unable to determine the global airflow direction of the fans.

Recommended Action: Execute the **copy support** command and contact your switch service provider.

PLAT-1009

Message: `Unable to read EEPROM Valid Signature for Global airflow direction.`

Message Type: LOG

Severity: ERROR

Probable Cause: Indicates that the content read from electrically erasable programmable read-only memory (EEPROM) is invalid and therefore unable to determine the global airflow direction of the fans.

Recommended Action: Execute the **copy support** command and contact your switch service provider.

PLAT-1011

Message: `Switch has older FPGA revision <Current FPGA revision>. FPGA revision <Available FPGA revision> is available.`

Message Type: LOG

Severity: WARNING

Probable Cause: Indicates that the firmware download command has downloaded a latest FPGA that is not activated yet.

This log is specific to platform EN4023 and Extreme VDX 2746. This log will not appear in other platforms.

Recommended Action: To activate the latest FPGA, power on reset the switch by doing one of the two steps: physically reseat the switch from the chassis or execute the command 'service -vr' from CMM CLI.

PLAT-1012

Message: `Switch has older FPGA revision <FPGA version already installed in HW>. The latest FPGA revision <FPGA version which NOS-Fusion carries> is available.`

Message Type: LOG

Severity: WARNING

Probable Cause: Indicates that the firmware download command has downloaded a latest FPGA that is not activated yet.

This log is specific to platform Fusion. This log will not appear in other platforms.

Recommended Action: It is highly recommended that FPGA be upgraded to the latest version.

To activate the latest FPGA, power on reset the switch: physically reseat the switch from the chassis

PLAT-1013

Message: `Linecard:<Latch Screws Status> Version:<Latch Screws Status>; Latch Screw Left:<Latch Screws Status> Right:<Latch Screws Status>`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that the 2 latch screws are installed or not

Recommended Action: No action is required.

PLAT-1014

Message: `Linecard:<Latch Optical Switch Feature Enabled/Disable> Latch Optical Switch Feature is <Latch Optical Switch Feature Enabled/Disable>.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that the latch optical switch feature is disabled or enabled

Recommended Action: No action is required.

PORT Messages

PORT-1003

Message: `Port <port number> Faulted because of many Link Failures.`

Message Type:LOG

Severity: WARNING

Probable Cause: Indicates that the specified port is disabled because of multiple link failures on the port that have exceeded the threshold internally set on the port. This problem is related to the hardware.

Recommended Action: Check and replace (if necessary) the hardware attached to both the ends of the specified port, including:

• The small form-factor pluggable (SFP)

• The cable (fiber-optic or copper inter-switch link (ISL))

• The attached devices

After checking the hardware, execute the **no shutdown** 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

Severity: INFO

Probable Cause: Indicates that the specified port cannot be enabled because other ports in the same group have used the buffers of this port group. This happens when other ports are configured to be long distance.

Recommended Action: To enable the specified port, perform one of the following actions:

• Reconfigure the other E_Ports so that they are not long distance.

• Change the other E_Ports so that they are not E_Ports.

This will free some buffers and allow the port to be enabled.

PORT-1011

Message: `An SFP transceiver for interface Fibre Channel <interface tuple string> is removed.`

Message Type:LOG

Severity: INFO

Probable Cause: Indicates that a small form-factor pluggable (SFP) transceiver has been removed from the specified port.

Recommended Action: No action is required.

PORT-1012

Message: `An SFP transceiver for interface Fibre Channel <interface tuple string> is inserted.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that a small form-factor pluggable (SFP) transceiver has been inserted into the specified port.

Recommended Action: No action is required.

PORT-1013

Message: `An incompatible SFP transceiver for interface Fibre Channel <interface tuple string> is inserted.`

Message Type:LOG

Severity: INFO

Probable Cause: Indicates that an incompatible small form-factor pluggable (SFP) transceiver has been inserted into the specified port.

Recommended Action: No action is required.

PORT-1014

Message: `Interface Fibre Channel <interface tuple string> is online.`

Message Type:LOG

Severity: INFO

Probable Cause: Indicates that the specified Fibre Channel interface has come online after the protocol dependencies are resolved.

Recommended Action: No action is required.

PORT-1015

Message: `Interface Fibre Channel <interface tuple string> is link down.`

Message Type:LOG

Severity: INFO

Probable Cause: Indicates that the specified Fibre Channel interface has gone offline because the link is down.

Recommended Action: Check whether the connectivity is proper and the remote link is up.

PORT-1016

Message: `Interface Fibre Channel <interface tuple string> is administratively up.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that the administrative status of the specified Fibre Channel interface has changed to up.

Recommended Action: No action is required.

PORT-1017

Message: `Interface Fibre Channel <interface tuple string> is administratively down.`

Message Type: LOG

Severity:INFO

Probable Cause: Indicates that the administrative status of the specified Fibre Channel interface has changed to down.

Recommended Action: No action is required.

QOSD Messages

QOSD-1000

Message: `QoS initialized successfully.`

Message Type:LOG

Severity:INFO

Probable Cause: Indicates that the Data Center Ethernet (DCE) QoS has been initialized.

Recommended Action: No action is required.

QOSD-1001

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

Message Type: LOG

Severity: ERROR

Probable Cause: Indicates that the specified function has failed to allocate memory.

Recommended Action: Check the memory usage on the switch using the **show process memory** command.

Restart or power cycle the switch.

QOSD-1005

Message: `QoS startup failed.`

Message Type:LOG

Severity:ERROR

Probable Cause: Indicates that Data Center Ethernet (DCE) QoS encountered an unexpected severe error during basic startup and initialization.

Recommended Action: Restart or power cycle the switch. If the problem persists, download a new firmware version using the **firmware download** command.

QOSD-1006

Message: `Interface <interface_name> is not allowed to come up as ISL because of Long Distance ISL restriction. Shutting down interface.`

Message Type:LOG

Severity:ERROR

Probable Cause: Indicates that the interface could not come up as inter-switch link (ISL) because only regular ISL is allowed for 2 Km and 5 Km distant links. The interface has been automatically shut down.

Recommended Action: No action is required.

QOSD-1007

Message: `sFlow profile <sflow-profile-name> is not present.`

Message Type:DCE

Severity:ERROR

Probable Cause: Indicates that the specified sFlow profile is not configured on the system.

Recommended Action: No action is required.

QOSD-1008

Message: `Classmap <class-map_name> is already applied on RBridge in dir <direction> through policy-map <policy-map_name>.`

Message Type: DCE

Severity:ERROR

Probable Cause: Indicates that the specified class-map is already applied on the RBridge.

Recommended Action: No action is required.

QOSD-1500

Message: `<BUM_protocol_name> traffic rate has been exceeded on interface <interface_name>.`

Message Type: DCE

Severity:INFO

Probable Cause: Indicates that the broadcast, unknown unicast, and multicast (BUM) monitor routine has detected a rate violation.

Recommended Action: No action is required.

QOSD-1501

Message: `<BUM_protocol_name> traffic rate returned to conforming on interface <interface_name>.`

Message Type:DCE

Severity:INFO

Probable Cause: Indicates that broadcast, unknown unicast, and multicast (BUM) storm control has detected that the traffic rate has returned to the normal limit on the specified interface.

Recommended Action: No action is required.

QOSD-1502

Message: `<BUM_protocol_name> traffic rate has been exceeded interface <interface_name>. Interface will be shut down.`

Message Type:DCE

Severity:INFO

Probable Cause: Indicates that the broadcast, unknown unicast, and multicast (BUM) monitor routine has detected a rate violation.

The interface has been shut down.

Recommended Action: Disable BUM storm control on the interface using the **no storm-control ingress** command; then re-enable the interface (using the **no shutdown** command) and BUM storm control

(using the **storm-control ingress** command).

QOSD-1503

Message: `The configured CIR/EIR is less than the minimum supported CIR/EIR (<MinSupportedInformationRate> bps) of this platform, the operational CIR/EIR will be 0.`

Message Type:DCE

Severity:INFO

Probable Cause: Indicates that the configured CIR/EIR is less than the supported operation range of platform results in complete drop of traffic matching the policer entry.

Recommended Action: No action is required.

QOSD-1600

Message: `Tail drops detected on interface <interface_name>.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that tail drops are detected on the specified interface.

Recommended Action: No action is required.

QOSD-1601

Message: `RED drops detected on interface <interface_name>.`

Message Type:DCE

Severity:INFO

Probable Cause: Indicates that red drops are detected on the specified interface.

Recommended Action: No action is required.

QOSD-1700

Message: Exceed QOS resources when adding member interface `<interface_name>` to lag `<Lag_name>`.

Message Type:DCE

Severity:INFO

Probable Cause: Space is not available on chip to create new `qos` maps.

Recommended Action: No action required.

QOSD-1800

Message: `Failed to inherit cos mutation map from parent lag <Lag_name> to member interface <interface_name>.`

Message Type:DCE

Severity:INFO

Probable Cause: Space is not available on chip to create new `qos` maps.

Recommended Action: No action is required.

QOSD-1801

Message: `Failed to inherit cos tc map from parent lag <Lag_name> to member interface <interface_name>.`

Message Type:DCE

Severity:INFO

Probable Cause: Space is not available on chip to create new `qos` maps.

Recommended Action: No action is required.

RADV Messages

RADV-1001

Message:`Inconsistent Curr Hop Limit Value <Local_router, Remote_router> received from router <router_name> on <router_name>`

Message Type: LOG

Severity: WARNING

Probable Cause: Indicates that the remote IPv6 router is configured with inconsistent values.

Recommended Action: Change the remote IPv6 router RA configuration to match with local router IPv6 RA configuration.

RADV-1002

Message:`Inconsistent M Flag Value <Local_router, Remote_router> received from <router_name> on <router_name>`

Message Type: LOG

Severity: WARNING

Probable Cause: Indicates that the remote IPv6 router is configured with inconsistent values.

Recommended Action: Change the remote IPv6 router RA configuration to match with local router IPv6 RA configuration.

RADV-1003

Message:`Inconsistent O Flag Value <Local_router, Remote_router> received from <router_name> on <router_name>`

Message Type: LOG

Severity: WARNING

Probable Cause: Indicates that the remote IPv6 router is configured with inconsistent values.

Recommended Action: Change the remote IPv6 router RA configuration to match with local router IPv6 RA configuration.

RADV-1004

Message:`Inconsistent Reachable Time Value <Local_router, Remote_router> received from <router_name> on <router_name>`

Message Type: LOG

Severity: WARNING

Probable Cause: Indicates that the remote IPv6 router is configured with inconsistent values.

Recommended Action: Change the remote IPv6 router RA configuration to match with local router IPv6 RA configuration.

RADV-1005

Message:`Inconsistent Retransmit Time Value <Local_router, Remote_router> received from <router_name> on <router_name>`

Message Type: LOG

Severity: WARNING

Probable Cause: Indicates that the remote IPv6 router is configured with inconsistent values.

Recommended Action: Change the remote IPv6 router RA configuration to match with local router IPv6 RA configuration.

RADV-1006

Message:`Inconsistent MTU Value <Local_router, Remote_router> received from <router_name> on <router_name>`

Message Type: LOG

Severity: WARNING

Probable Cause: Indicates that the remote IPv6 router is configured with inconsistent values.

Recommended Action: Change the remote IPv6 router RA configuration to match with local router IPv6 RA configuration.

RADV-1007

Message:`Valid lifetime value <Preferred_value, Valid_value> for prefix <%s/%d> received from <router_name> on <router_name>`

Message Type: LOG

Severity: WARNING

Probable Cause: Indicates that the remote IPv6 router is configured with inconsistent values.

Recommended Action: Change the remote IPv6 router RA configuration to match with local router IPv6 RA configuration.

RADV-1008

Message:`Inconsistent On-Link Flag Value <Local_router, Remote_router> for prefix (%s/%d) received from <router_name> on <router_name>.`

Message Type: LOG

Severity: WARNING

Probable Cause: Indicates that the remote IPv6 router is configured with inconsistent values.

Recommended Action: Change the remote IPv6 router RA configuration to match with local router IPv6 RA configuration.

RADV-1009

Message:`Inconsistent Auto Addr-Config Flag Value <Local_router, Remote_router> for prefix (%s/%d) received from <router_name> on <router_name>`

Message Type: LOG

Severity: WARNING

Probable Cause: Indicates that the remote IPv6 router is configured with inconsistent values.

Recommended Action: Change the remote IPv6 router RA configuration to match with local router IPv6 RA configuration.

RADV-1010

Message:`Inconsistent Preferred Lifetime Value <Local_router, Remote_router> for prefix (%s/%d) received from <router_name> on <router_name>`

Message Type: LOG

Severity: WARNING

Probable Cause: Indicates that the remote IPv6 router is configured with inconsistent values.

Recommended Action: Change the remote IPv6 router RA configuration to match with local router IPv6 RA configuration.

RADV-1011

Message:`Inconsistent Valid Lifetime Value <Local_router, Remote_router> for prefix (%s/%d) received from <router_name> on <router_name>`

Message Type: LOG

Severity: WARNING

Probable Cause: Indicates that the remote IPv6 router is configured with inconsistent values.

Recommended Action: Change the remote IPv6 router RA configuration to match with local router IPv6 RA configuration.

RADV-1006

Message:`Inconsistent MTU Value <Local_router, Remote_router> received from <router_name> on <router_name>`

Message Type: LOG

Severity: WARNING

Probable Cause: Indicates that the remote IPv6 router is configured with inconsistent values.

Recommended Action: Change the remote IPv6 router RA configuration to match with local router IPv6 RA configuration.

RAS Messages

RAS-1001

Message:`First failure data capture (FFDC) event occurred.`

Message Type: LOG

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 **`copy support`** 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

Severity:WARNING

Probable Cause: Indicates that the storage size for first failure data capture (FFDC) has reached the maximum.

Recommended Action: Execute the **`copy support`** command and contact your switch service provider.

RAS-1004

Message: `Software 'verify' error detected.`

Message Type:LOG | FFDC

Severity:WARNING

Probable Cause: Indicates an internal software error.

Recommended Action: Execute the **`copy support`** command and contact your switch service provider.

RAS-1005

Message: `Software 'assert' error detected.`

Message Type:LOG | FFDC

Severity:WARNING

Probable Cause: Indicates an internal software error.

Recommended Action: Execute the **copy support** 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

Severity:INFO

Probable Cause: Indicates that the support data was automatically transferred from the switch to the configured remote server.

Recommended Action: No action is required.

RAS-1007

Message: `System is about to reload.`

Message Type:LOG

Severity:INFO

Probable Cause: Indicates that the system reload was initiated.

Recommended Action: No action is required.

RAS-1008

Message: `Software detected OOM: module id <Module id> failed to allocate <Memory size> byte(s) of memory.`

Message Type: LOG | FFDC

Severity: WARNING

Probable Cause: Indicates that the system ran out of memory.

Recommended Action: Execute the **copy support** command and contact your switch service provider.

RAS-2001

Message: `Audit message log is enabled.`

Message Type:LOG | AUDIT

Class:RAS

Severity:INFO

Probable Cause: Indicates that the audit message log has been enabled.

Recommended Action: No action is required.

RAS-2002

Message: `Audit message log is disabled.`

Message Type:LOG | AUDIT

Class:RAS

Severity:INFO

Probable Cause: Indicates that the audit message log has been disabled.

Recommended Action: No action is required.

RAS-2003

Message: `Audit message class configuration has been changed to <New audit class configuration>.`

Message Type:LOG | AUDIT

Class:RAS

Severity:INFO

Probable Cause: Indicates that the audit event class configuration has been changed.

Recommended Action: No action is required.

RAS-2004

Message: `prom access is enabled.`

Message Type:LOG | AUDIT

Class:SECURITY

Severity:INFO

Probable Cause: Indicates that the PROM access has been enabled.

Recommended Action: No action is required.

RAS-2005

Message: `prom access is disabled.`

Message Type:LOG | AUDIT

Class:SECURITY

Severity:INFO

Probable Cause: Indicates that the PROM access has been disabled.

Recommended Action: No action is required.

RAS-2006

Message: `Audit log message storage has wrapped around.`

Message Type:LOG | AUDIT

Class:RAS

Severity:INFO

Probable Cause: Indicates that audit log message storage has wrapped around.

Recommended Action: No action is required.

RAS-2007

Message: `Audit log message storage has reached 75 percentage of limit.`

Message Type:LOG | AUDIT

Class:RAS

Severity:INFO

Probable Cause: Indicates that audit log message storage is 75% full.

Recommended Action: No action is required.

RAS-3001

Message: `USB storage device plug-in detected.`

Message Type:LOG

Severity:INFO

Probable Cause: Indicates that the USB storage device plug-in has been detected.

Recommended Action: No action is required.

RAS-3002

Message: `USB storage device enabled.`

Message Type:LOG

Severity:INFO

Probable Cause: Indicates that the USB storage device has been enabled.

Recommended Action: No action is required.

RAS-3003

Message: `USB storage device was unplugged before it was disabled.`

Message Type:LOG

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 usb off command before unplugged it from the system.

RAS-3004

Message: `USB storage device disabled.`

Message Type:LOG

Severity:INFO

Probable Cause: Indicates that the USB storage device has been disabled.

Recommended Action: No action is required.

RAS-3005

Message: `File <filename/directory> removed from USB storage.`

Message Type:LOG

Severity:INFO

Probable Cause: Indicates that the specified file or directory has been removed from the USB storage.

Recommended Action: No action is required.

RAS-3006

Message: `Log messages have been blocked from displaying on console for <Number of minutes> minutes.`

Message Type:LOG

Severity:INFO

Probable Cause: Indicates that the RASLog messages were disabled from displaying on the console for the specified duration by using the **`logging raslog console stop`** [*`minutes`*] command.

Recommended Action: No action is required.

RAS-3007

Message: `Logging messages to console has been enabled.`

Message Type:LOG

Severity:INFO

Probable Cause: Indicates that the RASLog console timer has expired.

Recommended Action: No action is required.

RAS-3008

Message: `Logging messages to console has been reset by user.`

Message Type:LOG

Severity:INFO

Probable Cause: Indicates that the RASLog messages were re-enabled to display on the console by using the **`logging raslog console start`** command.

Recommended Action: No action is required.

RAS-3009

Message: `Please log out all of the CLI sessions and log back in before enabling the USB storage device.`

Message Type:LOG

Severity:WARNING

Probable Cause: User sessions created after usb is turned on needs to be logged out once usb is turned off.

Recommended Action: Please log out of all user sessions. The **`show user`** command can be used to check for active user sessions.

RPS Messages

RPS-1001

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

Message Type: DCE

Severity: ERROR

Probable Cause: Indicates that the specified function has failed to allocate memory.

Recommended Action: Check the memory usage on the switch using the show process memory command.

Reload or power cycle the switch.

RPS-1750

Message:`Route Map <Route_map_name> is bound on interface <interface_name>.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that the specified route map has been applied to the specified interface.

Recommended Action: No action is required.

RPS-1751

Message: `Route Map <Route_map_name> binding on interface <interface_name> failed.`

Message Type: DCE

Severity: ERROR

Probable Cause: Indicates that the specified route map was not instantiated on the specified interface.

Recommended Action: No action is required.

RPS-1752

Message: `Route Map <Route_map_name> is unbound from interface <interface_name>.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that the specified route map has been removed from the specified interface.

Recommended Action: No action is required.

RPS-1753

Message: `Route Map <Route_map_name> unbinding from interface <interface_name> failed.`

Message Type: DCE

Severity: ERROR

Probable Cause: Indicates that the specified route map was not removed from the specified interface.

Recommended Action: No action is required.

RPS-1754

Message: `Route Map <Route_map_name> stanza sequence number <Stanza_sequence_number> binding to interface <interface_name> failed.`

Message Type: DCE

Severity: ERROR

Probable Cause: Indicates that a newly created stanza on an already active route map was unable to be instantiated.

Recommended Action: No action is required.

RTM Messages

RTM-1001

Message:`Initialization error: <messsage>.`

Message Type:DCE

Severity:ERROR

Probable Cause: Indicates that the route management (RTM) has encountered an error during initialization.

Recommended Action: Reload or power cycle the switch.

RTM-1002

Message: `RTM(<messsage>): Max route limit(<maximum limit>) reached.`

Message Type:DCE

Severity:ERROR

Probable Cause: Indicates that the route management (RTM) has reached its maximum capacity.

Recommended Action: Reduce the number of routes or next hops using the **`clear ip route`** command.

RTM-1022

Message: `Clear Routes success.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that IP routes are cleared by the route management (RTM).

Recommended Action: No action is required.

RTM-1032

Message: `System <messsage> Route Limits exceeded. Current Profile Routes Limit <routes limit>. Configured Routes <configured routes>.`

Message Type: DCE

Severity:ERROR

Probable Cause: Indicates system limits have exceeded.

Recommended Action:execute clear on all vrfs.

RTM-1033

Message: `System Next-Hop limits exceeded. Current Profile Nexthop <profile nexthop>. Configured Next-Hops <configured nexthops>.`

Message Type: DCE

Severity:ERROR

Probable Cause: Indicates that the route management (RTM) has reached its maximum nexthop capacity.

Recommended Action: Reduce the number of routes or next hops using the **`clear ip route`** command.

RTM-1037

Message: `<messsage>`

Message Type: DCE

Severity:INFO

Probable Cause: Indicates Graceful Restart Done.

Recommended Action: No action is required.

RTM-1039

Message: `[ IPv6 | IPv4 ] Hosts have reached the high threshold limit of <high-threshold-value>.`

Message Type: INFO

Severity: INFO

Probable Cause: The number of IPv6/IPv4 hosts in the ARP table has reached the user configured high threshold limit.

Recommended Action: Reduce the number of hosts stored in the table.

RTM-1040

Message: `[ IPV6 | IPv4 ] Hosts have dropped below the low threshold limit of <low-threshold-value >.`

Message Type: INFO

Severity: INFO

Probable Cause: The number of IPv6/IPv4 hosts in the ARP table has dropped below the user configured low threshold limit.

Recommended Action: No action is required.

RTM-1041

Message: `Nexthops have reached the high threshold limit of {high-threshold-limit}`

Message Type: INFO

Severity: INFO

Probable Cause: The number of nexthop entries has reached or exceeded the user configured high threshold level.

Recommended Action: Reduce the number of entries stored in the table.

RTM-1042

Message: `Nexthops have dropped below the user configured low threshold limit of {low-threshold-limit}`

Message Type: INFO

Severity: INFO

Probable Cause: The number of nexthop entries has dropped below the user configured low threshold level.

Recommended Action: No action is required.

SCN Messages

SCN-1001

Message: `SCN queue overflow for process <daemon name>.`

Message Type: FFDC | LOG

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

- webd
- 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 reload the switch. In this case, execute the copy support ftp command to send the core files using FTP to a secure server location.

If the message persists, execute the copy support command and contact your switch service provider.

SEC Messages

SEC-1033

Message: `Invalid character used in member parameter to add switch to SCC policy; command terminated.`

Message Type:LOG

Severity:ERROR

Probable Cause: Indicates that a member parameter in the secpolicy defined-policy command is invalid (for example, it may include an invalid character, such as an asterisk). A valid switch identifier (WWN, or switch name) must be provided as a member parameter in the **`secpolicy defined-policy`** command.

Recommended Action: Execute the **`secpolicy defined-policy`** command using a valid switch identifier (WWN, or switch name) to add specific switches to the switch connection control (SCC) policy.

SEC-1034

Message: `Invalid member <policy member>.`

Message Type:LOG

Severity:ERROR

Probable Cause: Indicates that the input list has an invalid member.

Recommended Action: Verify the member names and input the correct information.

SEC-1036

Message: `Device name <device name> is invalid due to a missing colon.`

Message Type:LOG

Severity:ERROR

Probable Cause: Indicates that one or more device names mentioned in the secpolicy defined-policy command does not have the colon character (:).

Recommended Action: Execute the **`secpolicy defined-policy`** command with a properly formatted device name parameter.

SEC-1037

Message: `Invalid WWN format <invalid WWN>.`

Message Type:LOG

Severity:ERROR

Probable Cause: Indicates that the World Wide Name (WWN) entered in the policy member list had an invalid format.

Recommended Action: Execute the command again using the standard WWN format, that is, 16 hexadecimal digits grouped as eight colon separated pairs. For example: 50:06:04:81:D6:F3:45:42.

SEC-1044

Message: `Duplicate member <member ID> in (<List>).`

Message Type:LOG

Severity:ERROR

Probable Cause: Indicates that 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 duplicate members.

SEC-1071

Message: `No new security policy data to apply.`

Message Type:LOG

Severity:ERROR

Probable Cause: Indicates that there are no changes in the defined security policy database to be activated.

Recommended Action: Verify that the security event was planned. Change some policy definitions and execute the secpolicy activate command to activate the policies.

SEC-1180

Message: `Added account <user name> with <role name> authorization.`

Message Type:LOG

Severity:INFO

Probable Cause: Indicates that the specified new account has been created.

Recommended Action: No action is required.

SEC-1181

Message: `Deleted account <user name>.`

Message Type:LOG

Severity:INFO

Probable Cause: Indicates that the specified account has been deleted.

Recommended Action: No action is required.

SEC-1184

Message: `<configuration> configuration change, action <action>, server ID <server>, VRF <vrf>.`

Message Type:LOG

Severity:INFO

Probable Cause: Indicates that the specified action is applied to remote AAA (RADIUS/TACACS+) server configuration. The possible actions are ADD, REMOVE, CHANGE, and MOVE.

Recommended Action: No action is required.

SEC-1185

Message: `<action> switch DB.`

Message Type:LOG

Severity:INFO

Probable Cause: Indicates that the switch database was enabled or disabled as the secondary authentication, authorization, and accounting (AAA) mechanism when the remote authentication dial-in user service (RADIUS) or Lightweight Directory Access Protocol (LDAP) is the primary AAA mechanism.

Recommended Action: No action is required.

SEC-1187

Message: `Security violation: Unauthorized switch <switch WWN> tries to join fabric.`

Message Type:LOG

Severity:INFO

Probable Cause: Indicates that a switch connection control (SCC) security violation was reported. The specified unauthorized switch attempts to join the fabric.

Recommended Action: Check the switch connection control policy (SCC) policy to verify the switches are 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 using the **`secpolicy defined-policy scc_policy member-entry`** command. 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-1189

Message: `Security violation: Unauthorized host with IP address <IP address> tries to do SNMP write operation.`

Message Type:LOG

Severity:INFO

Probable Cause: Indicates that a Simple Network Management Protocol (SNMP) security violation was reported. The specified unauthorized host attempted to perform an SNMP write operation.

Recommended Action: Check the WSNMP policy (read/write SNMP 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

Severity:INFO

Probable Cause: Indicates that a Simple Network Management Protocol (SNMP) security violation was reported. The specified unauthorized host attempted to perform an SNMP read operation.

Recommended Action: Check the RSNMP policy (read-only SNMP policy) to verify the hosts that are 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

Severity:INFO

Probable Cause: Indicates that a Hypertext Transfer Protocol (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

Severity:INFO

Probable Cause: Indicates that a serial or modem login security violation was reported. An incorrect password was used while trying to log in through a serial or modem connection; the log in 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

Severity:INFO

Probable Cause: Indicates that a login security violation was reported. The wrong password was used while trying to log in through the specified connection method; the log in failed. The violating IP address is displayed in the message.

Recommended Action: Verify that the specified IP address is being used by a valid switch administrator. Use the correct password.

SEC-1197

Message: `Changed account <user name>.`

Message Type:LOG

Severity:INFO

Probable Cause: Indicates that the specified account has changed.

Recommended Action: No action is required.

SEC-1199

Message: `Security violation: Unauthorized access to serial port of switch <switch instance>.`

Message Type:LOG

Severity:INFO

Probable Cause: Indicates that 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 was made on the console. If so, add the switch World Wide Name (WWN) to the serial policy using the secpolicy defined-policy scc_policy member-entry command. 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-1203

Message: `Login information: Login successful via TELNET/SSH/RSH. IP Addr: <IP address>.`

Message Type: LOG

Severity:INFO

Probable Cause: Indicates that the remote log in of the specified IP address was successful.

Recommended Action: No action is required.

SEC-1204

Message: `Root access mode is configured to <Mode>.`

Message Type:LOG

Severity: INFO

Probable Cause: Indicates that the root access mode is changed.

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-1205

Message: `Login information: User [<User>] Last Successful Login Time : <last_successful_login_time> and Fail count : <fail_count>.`

Message Type:LOG

Severity: INFO

Probable Cause: Indicates the last successful login time and the failed attempt count for the specified user.

Recommended Action: No action is required.

SEC-1206

Message: `Login information: User [<User>] Last Successful Login Time : <last_successful_login_time>.`

Message Type:LOG

Severity: INFO

Probable Cause: Indicates the last successful login time for the specified user.

Recommended Action: No action is required.

SEC-1307

Message: `<RADIUS/TACACS+/LDAP server identity> server <server> authenticated user account '<username>'.`

Message Type:LOG

Severity: INFO

Probable Cause: Indicates that the specified AAA (RADIUS/TACACS+/LDAP) server responded to a switch request after some servers timed out.

Recommended Action: If the message appears frequently, reconfigure the list of servers so that the responding server is the first server on the list.

SEC-1308

Message: `All <RADIUS/TACACS+/LDAP server identity> servers failed to authenticate user account '<username>'.`

Message Type:LOG

Severity: INFO

Probable Cause: Indicates that all servers in the remote AAA (RADIUS/TACACS+/LDAP) service configuration have failed to respond to a switch request within the configured timeout period.

Recommended Action: Verify that the switch has proper network connectivity to the specified AAA (RADIUS/TACACS+/LDAP) servers and the servers are correctly configured.

SEC-1312

Message: `passwdcfg params changed as (<changed param>:<old value> -> <new value>).`

Message Type:LOG

Severity: INFO

Probable Cause: Indicates that the password attributes have been changed.

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-1313

Message: `The password attributes parameters were set to default values.`

Message Type:LOG

Severity: INFO

Probable Cause: Indicates that the password attributes were set to default values.

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-1325

Message: `Security enforcement: Switch <switch WWN> connecting to port <Port number> is not authorized to stay in fabric.`

Message Type:LOG

Severity:ERROR

Probable Cause: Indicates that the specified switch is being disabled on the specified port because of a switch connection control (SCC) policy violation.

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 using the **`secpolicy defined-policy scc_policy member-entry`** command, then attempt to join the switch with the fabric.

SEC-1329

Message: `IPFilter enforcement:Failed to enforce ipfilter policy of <Policy Type> type because of <Error code>.`

Message Type:LOG

Severity:ERROR

Probable Cause: Indicates that the IP filter policy enforcement failed because of an internal system failure.

Recommended Action: Execute the **`copy support`** command and contact your switch service provider.

SEC-1334

Message: `local security policy <Event name>.`

Message Type:LOG

Severity: INFO

Probable Cause: Indicates that the specified event has occurred.

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.

SEC-1335

Message: `local security policy <Event name> WWN <Member WWN>.`

Message Type:LOG

Severity: INFO

Probable Cause: Indicates that the specified event has occurred.

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.

SEC-1336

Message: `Missing file <file name> is replaced with default configuration.`

Message Type:LOG

Severity: INFO

Probable Cause: Indicates that the specified file is missing and it has been replaced with the default file.

Recommended Action: No action is required.

SEC-1337

Message: `Failed to access file <file name> and reverted the configuration.`

Message Type:LOG

Severity: INFO

Probable Cause: Indicates that the specified file was not accessible.

Recommended Action: No action is required.

SEC-1338

Message: `Accounting message queue 90 percent full, some messages may be dropped.`

Message Type:LOG

Severity:WARNING

Probable Cause: Cause Indicates that the server is unreachable.

Recommended Action: No action is required.

SEC-1339

Message: `Accounting message queue within limits all messages will be processed.`

Message Type:LOG

Severity: INFO

Probable Cause: Indicates that the server is now reachable.

Recommended Action: No action is required.

SEC-1340

Message: `All TACACS+ servers failed to account user activity. Status is <return_status>`

Message Type:LOG

Severity: INFO

Probable Cause: Indicates that the accounting has failed

Recommended Action: Check secret key value.

SEC-1341

Message: `Security violation: Login failure attempt outside the access time via <connection method>.`

Message Type:LOG

Severity: INFO

Probable Cause: Indicates that a serial or modem login security violation was reported. User attempted to login outside the access time window through the specified connection method; the log in failed.

Recommended Action: Verify the login access time for the user. If needed update the access time as required.

SEC-1342

Message: `Security violation: Login failure attempt outside access time by user [<user>] via <connection method>. IP Addr: <IP address>.`

Message Type:LOG

Severity: INFO

Probable Cause: Indicates that a login security violation was reported. User attempted to login outside the access time window through the specified connection method; the log in failed.

Recommended Action: Verify the login access time for the user. If needed update the access time as required.

SEC-1343

Message: `All RADIUS servers failed to account user activity. Status is <return_status>.`

Message Type:LOG

Severity: INFO

Probable Cause: Indicates that the accounting has failed.

Recommended Action: Check secret key value.

SEC-3014

Message: `Event: <Event Name>, Status: success, Info: <Event related info> <Event option> server <Server Name> vrf <VRF> for AAA services.`

Message Type:AUDIT

Class:SECURITY

Severity: INFO

Probable Cause: Indicates that the AAA (RADIUS/TACACS+) server configuration has been changed manually.

Recommended Action: Verify that the RADIUS/TACACS+ configuration was changed intentionally. If the RADIU/TACACS+ configuration was changed intentionally, no action is required. If the RADIUS/TACACS+ configuration was not changed intentionally, take appropriate action as defined by your enterprise security policy.

SEC-3016

Message: `Event: <Event Name>, Status: success, Info: Attribute [<Attribute Name>] of <Attribute related info> server <server ID> vrf <VRF> changed <Attribute related info, if any>.`

Message Type:AUDIT

Class:SECURITY

Severity: INFO

Probable Cause: Indicates that the specified attribute of the remote AAA (RADIUS/TACACS+) server has been changed manually.

Recommended Action: Verify that the attribute was changed intentionally. If the attribute was changed intentionally, no action is required. If the attribute was not changed intentionally, 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 to New Value>.`

Message Type: AUDIT

Class:SECURITY

Severity: INFO

Probable Cause: Indicates that the specified password attribute has been changed.

Recommended Action: Verify that the password attribute was changed intentionally. If the password attribute was changed intentionally, no action is required. If the password attribute was not changed intentionally, take appropriate action as defined by your enterprise security policy.

SEC-3019

Message: `Event: <Event Name>, Status: success, Info: Password attributes set to default values.`

Message Type:AUDIT

Class:SECURITY

Severity: INFO

Probable Cause: Indicates that the password attributes are set to default values.

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-3020

Message: `Event: <Event Name>, Status: success, Info: Successful login attempt via <connection method and IP Address>.`

Message Type: AUDIT

Class:SECURITY

Severity: INFO

Probable Cause: Indicates that the log in was successful. An IP address is displayed when the login occurs over a remote connection.

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-3021

Message: `Event: <Event Name>, Status: failed, Info: Failed login attempt through <connection method and IP Address>.`

Message Type:AUDIT

Class:SECURITY

Severity: INFO

Probable Cause: Indicates that the log in attempt has failed.

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-3022

Message: `Event: <Event Name>, Status: success, Info: Successful logout by user [<User>].`

Message Type:AUDIT | LOG

Class:SECURITY

Severity: INFO

Probable Cause: Indicates that the specified user has successfully logged out.

Recommended Action: No action is required.

SEC-3023

Message: `Event: <Event Name>, Status: failed, Info: Account [<User>] locked, failed password attempts exceeded.`

Message Type:AUDIT

Class:SECURITY

Severity: INFO

Probable Cause: Indicates that the number of failed log in attempts due to incorrect password has exceeded the allowed limit; the account has been locked.

Recommended Action: The administrator can manually unlock the account.

SEC-3024

Message: `Event: <Event Name>, Status: success, Info: User account [<User Name>], password changed.`

Message Type: AUDIT

Class:SECURITY

Severity: INFO

Probable Cause: Indicates that the password was changed for the specified user.

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-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

Class:SECURITY

Severity: INFO

Probable Cause: Indicates that a new user account was created.

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-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

Class:SECURITY

Severity: INFO

Probable Cause: Indicates that the user account role has been changed.

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-3027

Message: `Event: <Event Name>, Status: success, Info: User account [<User Name>] [<Changed Attributes>].`

Message Type: AUDIT

Class:SECURITY

Severity: INFO

Probable Cause: Indicates that the user account properties were changed.

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-3028

Message: `Event: <Event Name>, Status: success, Info: User account [<User Name>] deleted.`

Message Type:AUDIT

Class:SECURITY

Severity: INFO

Probable Cause: Indicates that the specified user account has been deleted.

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-3030

Message: `Event: <Event Name>, Status: success, Info: <Event Specific Info>.`

Message Type:AUDIT

Class:SECURITY

Severity: INFO

Probable Cause: Indicates that the certificate authority (CA) certificate was imported successfully using the **`certutil import ldapca`** command.

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-3034

Message: `Event: AAA Authentication Login Mode Configuration, Status: success, Info: Authentication configuration changed from <Previous Mode> to <Current Mode>.`

Message Type: AUDIT

Class:SECURITY

Severity: INFO

Probable Cause: Indicates that the authentication configuration has been changed.

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-3035

Message: `Event: ipfilter, Status: success, Info: <IP Filter Policy> ipfilter policy(ies) saved.`

Message Type:AUDIT | LOG

Class:SECURITY

Severity: INFO

Probable Cause: Indicates that the specified IP filter policies have been saved.

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-3036

Message: `Event: ipfilter, Status: failed, Info: Failed to save changes for <IP Filter Policy> ipfilter policy(s).`

Message Type: AUDIT | LOG

Class:SECURITY

Severity: INFO

Probable Cause: Indicates that the specified IP filter policies have not been saved.

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-3037

Message: `Event: ipfilter, Status: success, Info: <IP Filter Policy> ipfilter policy activated.`

Message Type:AUDIT | LOG

Class:SECURITY

Severity: INFO

Probable Cause: Indicates that the specified IP filter policy has been activated.

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-3038

Message: `Event: ipfilter, Status: failed, Info: Failed to activate <IP Filter Policy> ipfilter policy.`

Message Type:AUDIT | LOG

Class:SECURITY

Severity: INFO

Probable Cause: Indicates that the specified IP filter policy failed to activate.

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-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

Class:SECURITY

Severity: INFO

Probable Cause: Indicates that 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-3045

Message: `Zeroization has been executed on the system.`

Message Type:AUDIT

Class:SECURITY

Severity: INFO

Probable Cause: Indicates that 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

Class:SECURITY

Severity: INFO

Probable Cause: Indicates that there was a change in the Federal Information Protection Standard (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-3049

Message: `Status of bootprom access is changed using prom-access disable CLI: <Access Status>.`

Message Type:AUDIT

Class:SECURITY

Severity: INFO

Probable Cause: Indicates that the status of Boot PROM has changed using prom-access disable command. By default, the Boot PROM is accessible.

Recommended Action: No action is required.

SEC-3051

Message: `The license key <Key> is <Action>.`

Message Type:AUDIT | LOG

Class:SECURITY

Severity: INFO

Probable Cause: Indicates that the specified license key has been added or removed.

Recommended Action: No action is required.

SEC-3061

Message: `Role '<Role Name>' is created.`

Message Type:AUDIT | LOG

Class:SECURITY

Severity: INFO

Probable Cause: Indicates that the specified role has been created.

Recommended Action: No action is required.

SEC-3062

Message: `Role '<Role Name>' is deleted.`

Message Type:AUDIT | LOG

Class:SECURITY

Severity: INFO

Probable Cause: Indicates that the specified role has been deleted.

Recommended Action: No action is required.

SEC-3067

Message: `Event: <Event Name>, Status: success, Info: Telnet Server is shutdown.`

Message Type: AUDIT

Class:SECURITY

Severity: INFO

Probable Cause: Indicates that the Telnet server in the switch is shut down.

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-3068

Message: `Event: <Event Name>, Status: success, Info: Telnet Server is started.`

Message Type:AUDIT

Class:SECURITY

Severity: INFO

Probable Cause: Indicates that the Telnet server in the switch is started.

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-3069

Message: `Event: <Event Name>, Status: success, Info: SSH Server is shutdown.`

Message Type: AUDIT

Class:SECURITY

Severity: INFO

Probable Cause: Indicates that the SSH server in the switch is shut down.

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-3070

Message: `Event: <Event Name>, Status: success, Info: SSH Server is started.`

Message Type: AUDIT

Class:SECURITY

Severity: INFO

Probable Cause: Indicates that the SSH server in the switch is started.

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-3071

Message: `Event: <Event Name>, Status: success, Info: SSH Server Key Exchange Algorithm is configured to DH Group 14.`

Message Type:AUDIT

Class:SECURITY

Severity: INFO

Probable Cause: Indicates that the SSH server key exchange algorithm is configured to DH group 14.

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-3072

Message: `Event: <Event Name>, Status: success, Info: SSH Server Key Exchange Algorithm is restored to default.`

Message Type:AUDIT

Class:SECURITY

Severity: INFO

Probable Cause: Indicates that the SSH server key exchange algorithm is restored to default.

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-3073

Message: `Event: <Event Name>, Status: success, Info: Login banner message is set to '<Banner>'.`

Message Type: AUDIT

Class:SECURITY

Severity: INFO

Probable Cause: Indicates that the login banner message is set.

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-3074

Message: `Event: <Event Name>, Status: success, Info: Login banner message is removed.`

Message Type: AUDIT

Class:SECURITY

Severity: INFO

Probable Cause: Indicates that the login banner message is removed.

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-3075

Message: `Event: <Event Name>, Status: success, Info: '<Type of cipher (LDAP/SSH)>' cipher list is configured.`

Message Type:AUDIT

Class:SECURITY

Severity: INFO

Probable Cause: Indicates that the specified Lightweight Directory Access Protocol (LDAP) or SSH cipher list is configured.

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-3076

Message: `Event: <Event Name>, Status: success, Info: '<Type of cipher (LDAP/SSH)>' cipher list is removed.`

Message Type:AUDIT

Class:SECURITY

Severity: INFO

Probable Cause: Indicates that the specified Lightweight Directory Access Protocol (LDAP) or SSH cipher list is removed.

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-3077

Message: `Event: <Event Name>, Status: success, Info: SSH Server Rekey Interval is configured to <RekeyInterval>.`

Message Type:AUDIT

Class:SECURITY

Severity: INFO

Probable Cause: Indicates that the SSH server periodic rekeying is enabled with configured interval.

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-3078

Message: `Event: <Event Name>, Status: success, Info: SSH Server Rekey Interval is removed.`

Message Type:AUDIT

Class:SECURITY

Severity: INFO

Probable Cause: Indicates that the SSH server periodic rekeying is disabled.

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-3079

Message: `Event: <Event Name>, Status: success, Info: SSH Server Cipher is configured to <Cipher>.`

Message Type:AUDIT

Class:SECURITY

Severity: INFO

Probable Cause: Indicates that the SSH server cipher is changed to configured value.

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-3080

Message: `Event: <Event Name>, Status: success, Info: SSH Server Cipher is restored to default.`

Message Type:AUDIT

Class:SECURITY

Severity: INFO

Probable Cause: Indicates that the SSH server cipher is restored to default.

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-3081

Message: `Event: <Event Name>, Status: success, Info: SSH Client Cipher is configured to <Cipher>.`

Message Type:AUDIT

Class:SECURITY

Severity: INFO

Probable Cause: Indicates that the SSH client cipher is changed to configured value.

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-3082

Message: `Event: <Event Name>, Status: success, Info: SSH Client Cipher is restored to default.`

Message Type:AUDIT

Class:SECURITY

Severity: INFO

Probable Cause: Indicates that the SSH client cipher is restored to default.

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-3083

Message: `Event: <Event Name>, Status: success, Info: Root access mode is restored to default (SSH/Telnet/Console).`

Message Type:AUDIT

Class:SECURITY

Severity: INFO

Probable Cause: Indicates that the root access mode is restored to default (SSH/Telnet/Console).

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-3084

Message: `Event: <Event Name>, Status: success, Info: Root access mode is configured to <mode>.`

Message Type:AUDIT

Class:SECURITY

Severity: INFO

Probable Cause: Indicates that the root access mode is changed to the configured value

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-3085

Message: `Event: <Event Name>, Status: success, Info: Root account is <status>.`

Message Type:AUDIT

Class:SECURITY

Severity: INFO

Probable Cause: Indicates that the root account is enabled or disabled.

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-3086

Message: `Event: <Event Name>, Status: success, Info: Standby Telnet server is <status>.`

Message Type:AUDIT

Class:SECURITY

Severity: INFO

Probable Cause: Indicates that the standby Telnet server in the switch is started or shutdown.

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-3087

Message: `Event: <Event Name>, Status: success, Info: Standby SSH server is <status>.`

Message Type:AUDIT

Class:SECURITY

Severity: INFO

Probable Cause: Indicates that the standby SSH server in the switch is started or shutdown.

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-3088

Message: `Event: <Event Name>, Status: success, Info: SSH <Key Type> Key <status>.`

Message Type:AUDIT

Class:SECURITY

Severity: INFO

Probable Cause: Indicates that the SSH key is generated or deleted.

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-3089

Message: `Event: <Event Name>, Status: success, Info: Crypto key is generated.`

Message Type:AUDIT

Class:SECURITY

Severity: INFO

Probable Cause: Indicates that the Crypto key is generated.

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-3090

Message: `Event: <Event Name>, Status: success, Info: Crypto key is deleted.`

Message Type:AUDIT

Class:SECURITY

Severity: INFO

Probable Cause: Indicates that the Crypto key is deleted.

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-3091

Message: `Event: <Event Name>, Status: success, Info: Crypto CA Trustpoint is created.`

Message Type:AUDIT

Class:SECURITY

Severity: INFO

Probable Cause: Indicates that the Crypto CA Trustpoint is created.

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-3092

Message: `Event: <Event Name>, Status: success, Info: Crypto CA Trustpoint is deleted.`

Message Type:AUDIT

Class:SECURITY

Severity: INFO

Probable Cause: Indicates that the Crypto CA Trustpoint is deleted.

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-3093

Message: `Event: <Event Name>, Status: success, Info: Crypto CA Trustpoint - Keypair associated.`

Message Type:AUDIT

Class:SECURITY

Severity: INFO

Probable Cause: Indicates that the Crypto CA Trustpoint and keypair are associated.

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-3094

Message: `Event: <Event Name>, Status: success, Info: Crypto CA Trustpoint - Keypair disassociated.`

Message Type:AUDIT

Class:SECURITY

Severity: INFO

Probable Cause: Indicates that the Crypto CA Trustpoint and keypair are disassociated.

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-3095

Message: `Event: <Event Name>, Status: success, Info: Crypto CA Trustpoint is authenticated.`

Message Type:AUDIT

Class:SECURITY

Severity: INFO

Probable Cause: Indicates that the CA certificate of the Crypto CA Trustpoint is imported.

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-3096

Message: `Event: <Event Name>, Status: success, Info: Crypto CA Trustpoint is unauthenticated.`

Message Type:AUDIT

Class:SECURITY

Severity: INFO

Probable Cause: Indicates that the CA certificate of the Crypto CA Trustpoint is deleted.

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-3097

Message: `Event: <Event Name>, Status: success, Info: Crypto CA Trustpoint is enrolled.`

Message Type:AUDIT

Class:SECURITY

Severity: INFO

Probable Cause: Indicates that the Crypto CA Trustpoint Certificate Signing Request (CSR) is generated and exported.

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-3098

Message: `Event: <Event Name>, Status: success, Info: Crypto CA Trustpoint certificate is imported.`

Message Type:AUDIT

Class:SECURITY

Severity: INFO

Probable Cause: Indicates that the Crypto CA Trustpoint identity certificate is imported.

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-3099

Message: `Event: <Event Name>, Status: success, Info: Crypto CA Trustpoint certificate is deleted.`

Message Type:AUDIT

Class:SECURITY

Severity: INFO

Probable Cause: Indicates that the Crypto CA Trustpoint identity certificate is deleted.

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-3100

Message: `Event: <Event Name>, Status: success, Info: SSH Server MAC is configured to <MAC>.`

Message Type:AUDIT

Class:SECURITY

Severity: INFO

Probable Cause: Indicates that the SSH server MAC is changed to the configured value

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-3101

Message: `Event: <Event Name>, Status: success, Info: SSH Client MAC is configured to <MAC>.`

Message Type:AUDIT

Class:SECURITY

Severity: INFO

Probable Cause: Indicates that the SSH client MAC is changed to the configured value.

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-3102

Message: `Event: <Event Name>, Status: success, Info: SSH Client Kex is configured to <Kex>.`

Message Type:AUDIT

Class:SECURITY

Severity: INFO

Probable Cause: Indicates that the SSH client Kex is changed to configured value

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-3103

Message: `Event: <Event Name>, Status: success, Info: SSH Server Key Exchange is configured to <Kex>.`

Message Type:AUDIT

Class:SECURITY

Severity: INFO

Probable Cause: Indicates that the SSH server key exchange (Kex) is changed to the configured value.

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-3104

Message: `Event: <Event Name>, Status: success, Info: SSH Server instance is started on <Vrfname> VRF.`

Message Type:AUDIT | LOG

Class:SECURITY

Severity: INFO

Probable Cause: Indicates that the SSH server instance is started on given VRF.

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-3105

Message: `Event: <Event Name>, Status: success, Info: SSH Server instance is stopped on <Vrfname> VRF.`

Message Type:AUDIT | LOG

Class:SECURITY

Severity: INFO

Probable Cause: Indicates that the SSH server instance is stopped on given VRF.

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-3106

Message: `Event: <Event Name>, Status: success, Info: Telnet Server instance is started on <Vrfname> VRF.`

Message Type:AUDIT

Class:SECURITY

Severity: INFO

Probable Cause: Indicates that the Telnet server instance is started on given VRF.

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-3107

Message: `Event: <Event Name>, Status: success, Info: Telnet Server instance is stopped on <Vrfname> VRF.`

Message Type:AUDIT

Class:SECURITY

Severity: INFO

Probable Cause: Indicates that the Telnet server instance is stopped on given VRF.

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-3108

Message: `Event: <Event Name>, Status: success, Info: SSH Server Port is configured to <ServerPort>.`

Message Type:AUDIT

Class:SECURITY

Severity: INFO

Probable Cause: Indicates that the SSH server is configured with a new port.

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-3110

Message: `Event: <Event Name>, <Event action> Info: <Even specific info>.`

Message Type:AUDIT | LOG

Class:SECURITY

Severity: INFO

Probable Cause: Indicates a failure to establish a Transport Layer Security (TLS) session.

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-3111

Message: `Event: <Event Name>, <Event action> Info: <Even specific info>.`

Message Type:AUDIT

Class:SECURITY

Severity: INFO

Probable Cause: Indicates TLS session information during connection.

Recommended Action: No action is required.

SEC-3112

Message: `Event: <Event Name>, <Event action> Info: <Even specific info>.`

Message Type:AUDIT | LOG

Class:SECURITY

Severity: INFO

Probable Cause: Indicates that Transport Layer Security (TLS) Certificate Validation failed.

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-3113

Message: `Event: <Event Name>, <Event action> Info: <Even specific info>.`

Message Type:AUDIT | LOG

Class:SECURITY

Severity: INFO

Probable Cause: Indicates SSH protocol message information during SSH session.

Recommended Action: No action is required.

SEC-3136

Message: `cert expiry , Alert-level:'<alert-level>', Certificate Details= '<certificate-details>' will expire in '<Days>' days.`

Message Type:AUDIT | LOG

Class:SECURITY

Severity: INFO

Probable Cause: Indicates that specified certificate will expire in the specified number of days.

Recommended Action: Certificate must be renewed to prevent issues due to certificate expiry.

SEC-3137

Message: `certificate expired, Certificate Details= '<certificate-details>' has expired '<Days>' days ago.`

Message Type:AUDIT | LOG

Class:SECURITY

Severity: INFO

Probable Cause: Indicates that specified certificate has expired the specified number of days in the past.

Recommended Action: Certificate must be renewed to continue using it.

SEC-3138

Message: `user inactivity warning, USER '<User-ID>' will expire in '<Days>' days.`

Message Type:AUDIT | LOG

Class:SECURITY

Severity: INFO

Probable Cause: Indicates that specified user account will expire in the specified number of days.

Recommended Action: Account must be used to login to the device to keep it active.

SEC-3139

Message: `user expired USER '<User-ID>' expired '<Days>' days ago.`

Message Type:AUDIT | LOG

Class:SECURITY

Severity: INFO

Probable Cause: Indicates that specified user account has expired the specified number of days ago.

Recommended Action: Account must be re-activated and used to login to the device.

SEC-3140

Message: `Event: user password expiry, Alert-level:< alert-level>, Password of user account <user-account> will expire in <number-of-days> days.`

Message Type:AUDIT | LOG

Severity: WARNING

Probable Cause: The user account specified in the <user-account> parameter will need to change their password in <number-of-days>.

Recommended Action: Change the user account's password before it expires.

SEC-3141

Message: `Event: user password expiring, Password of user account <user-account> is expiring today.`

Message Type:AUDIT | LOG

Severity: ERROR

Probable Cause: The password for user account specified in the <user-account> parameter will expire at the end of the current day. The user has to change the password immediately. If not changed, the password will expire.

Recommended Action: Change the user account's password before it expires.

SEC-3142

Message: `Event: user password expired, Password of user account <user-account> has expired <number-of-days> days ago.`

Message Type:AUDIT | LOG

Severity: ERROR

Probable Cause: The user account specified in the <user-account> parameter is locked out and will need to change their password immediately to log in.

Recommended Action: Change the user account's password immediately.

SEC-3501

Message: `Role '<Role Name>' is changed.`

Message Type:AUDIT | LOG

Class:SECURITY

Severity: INFO

Probable Cause: Indicates that attributes of the specified role have been changed.

Recommended Action: No action is required.

SEC-4002

Message: `Event: <Event Name>, Status: failed, Info: Failed login attempt outside the access time through <connection method and IP Address>.`

Message Type:AUDIT

Class:SECURITY

Severity: INFO

Probable Cause: Indicates that the log in attempt outside the access time has failed.

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.

SFLO Messages

SFLO-1001

Message:`sFlow is <state> globally.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that sFlow is enabled or disabled globally.

Recommended Action: No action is required.

SFLO-1002

Message: `sFlow is <state> for port <name>.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that sFlow is enabled or disabled on the specified port.

Recommended Action: No action is required.

SFLO-1003

Message: `Global sFlow sampling rate is changed to <sample_rate>.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that the global sFlow sampling rate has been changed to the specified value.

Recommended Action: No action is required.

SFLO-1004

Message: `Global sFlow polling interval is changed to <polling_intvl>.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that the global counter sampling interval has been changed to the specified value.

Recommended Action: No action is required.

SFLO-1005

Message: `sFlow sampling rate on port <name> is changed to <sample_rate>.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that the sFlow sampling rate has been changed on the specified port.

Recommended Action: No action is required.

SFLO-1006

Message: `sFlow polling interval on port <name> is changed to <poling_intvl>.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that the sFlow polling interval has been changed on the specified port.

Recommended Action: No action is required.

SFLO-1007

Message: `<name> is <state> as sFlow collector.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that the specified sFlow collector is either configured or not configured.

Recommended Action: No action is required.

SFLO-1008

Message: `All the sFlow collectors are unconfigured.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that none of the sFlow collectors are configured.

Recommended Action: No action is required.

SFLO-1009

Message: `Socket Operation Failed while connecting with the collector address.`

Message Type: DCE

Severity:WARNING

Probable Cause: Indicates that the connection to the sFlow collector server failed.

Recommended Action: Reconfigure the sFlow collector using the **`sflow collector`** command.

SFLO-1010

Message: `sFlow profile is created with name <name> and sampling rate <sample_rate>.`

Message Type: DCE

Severity:INFO

Probable Cause: Indicates that the specified sFlow profile has been created.

Recommended Action: No action is required.

SFLO-1011

Message: `sFlow profile with name <name> is deleted.`

Message Type: DCE

Severity:INFO

Probable Cause: Indicates that the specified sFlow profile has been deleted.

Recommended Action: No action is required.

SFLO-1012

Message: `sFlow profile with name <name> is updated with sampling rate <sample_rate>.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that the sampling rate has been updated for the specified sFlow profile.

Recommended Action: No action is required.

SFLO-1013

Message: `sFlow profile with name <name> is in use. Cannot be deleted.`

Message Type: DCE

Severity:WARNING

Probable Cause: Indicates that the specified sFlow profile is in use and therefore it cannot be deleted.

Recommended Action: No action is required.

SFLO-1014

Message: `<INFO %s>.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates the sFlow configuration details.

Recommended Action: No action is required.

SFLO-1015

Message: `Max no. of profiles (<message>) already configured.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates the sFlow configuration details.

Recommended Action: No action is required.

SFLO-1016

Message: `sFlow Collector VRF is changed to <vrf_name>.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that sFlow collector VRF has been changed to the specified value.

Recommended Action: No action is required.

SFLO-1017

Message: `sFlow null0 sampling is <state> globally.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that sFlow null0 sampling is enabled or disabled globally.

Recommended Action: No action is required.

SFLO-1018

Message: `sFlow SourceIP Interface is changed to <srcIpIfTypeStr> <srcIpIfNumStr> (<srcIpIfOsName>).`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that sFlow SourceIP Interface has been changed to the specified value.

Recommended Action: No action is required.

SFLO-1019

Message: `sFlow Agent address is changed to <agentAddrTypeStr>, Intf: <agentAddrIfTypeStr> <agentAddrIfNumStr> (<agentAddrIfOsName>).`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that sFlow Agent address has been changed to the specified value.

Recommended Action: No action is required.

SFLO-1021

Message: `Updating of destination MAC in sFlow samples for routed packets is enabled globally.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that updating destination MAC in sFlow sames for routed packets is enabled globally.

Recommended Action: No action is required.

SFLO-1022

Message: `Updating of destination MAC in sFlow samples for routed packets is disabled globally.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that updating destination MAC in sFlow sames for routed packets is disabled globally.

Recommended Action: No action is required.

SLCD Messages

SLCD-1001

Message:`CF life percentage used up is between 90 - 95 on card No. <CF Card number in integer>, Actual percentage <life span of CF used up in percentage>.`

Message Type: LOG

Severity: WARNING

Probable Cause: Indicates that the compact flash (CF) life span left over is a little more than 5 percent as reported by the CF wear leveling statistics.

Recommended Action: The CF card must be replaced as soon as possible. Contact your switch service provider for the CF card replacement.

SLCD-1002

Message: `CF life span percentage is between 95 - 99 on card No. <CF Card number in integer>, Actual percentage <Life span used up on CF in percentage>.`

Message Type: LOG

Severity: WARNING

Probable Cause: Indicates that the compact flash (CF) life span left over is between 1 and 5 percent as reported by the CF wear leveling statistics.

Recommended Action: The CF card must be replaced immediately for proper functioning. Contact your switch service provider for the CF card replacement.

SLCD-1003

Message: `CF life span percentage left is less than 1 on card No. <CF Card number in integer>, Actual percentage <Life span used up on CF card in percentage>.`

Message Type: LOG

Severity: ERROR

Probable Cause: Indicates that the compact flash (CF) life span left over is less than 1 percent as reported by the CF wear leveling statistics.

Recommended Action: A new CF card is required for proper functioning of the chassis. Contact your switch service provider for the CF card replacement.

SLCD-1004

Message: `CF life span percentage left on Card No <CF Card number in integer> is - <Life span left on CF card in percentage>.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates the available life span of the compact flash (CF) as reported by the CF wear leveling statistics.

Recommended Action: No action is required.

SLCD-1005

Message: `Spare Blocks percentage left on Card No. <CF Card number in integer> is between 5-10,Actual percentage is - <Spare Blocks left in percentage>.`

Message Type: LOG

Severity:WARNING

Probable Cause: Indicates that the spare blocks percentage left on the compact flash (CF) card is between 5 and 10 percent as reported by the CF wear leveling statistics.

Recommended Action: The CF card must be replaced as soon as possible. Contact your switch service provider for the CF card replacement.

SLCD-1006

Message: `Spare Blocks percentage left on CF Card No. <CF Card number in integer> is between 1-5,Actual percentage is - <Spare Blocks left in percentage>.`

Message Type: LOG

Severity: WARNING

Probable Cause: Indicates that the spare blocks percentage left on the compact flash (CF) card is between 1 and 5 percent as reported by the CF wear leveling statistics.

Recommended Action: The CF card must be replaced immediately for proper functioning. Contact your switch service provider for the CF card replacement.

SLCD-1007

Message: `Spare Blocks percentage left on CF Card No. <CF Card number in integer> are less than 1,Actual percentage is - <Spare Blocks left in percentage>.`

Message Type: LOG

Severity: WARNING

Probable Cause: Indicates that the spare blocks percentage left on the compact flash (CF) card is less than 1 percent as reported by the CF wear leveling statistics.

Recommended Action: A new CF card is required for proper functioning of the chassis. Contact your switch service provider for the CF card replacement.

SLCD-1008

Message: `Spare Blocks percentage left on CF Card No. <CF Card number in integer> are - <Spare Blocks left in percentage>.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates the percentage of the spare blocks left on the compact flash (CF) card as reported by the CF wear leveling statistics.

Recommended Action: No action is required.

SLCD-1009

Message: `Unable to get Wear leveling stats for CF card No. <CF Card number in integer>.`

Message Type: LOG

Severity: ERROR

Probable Cause: Indicates that wear leveling data cannot be retrieved from the attached compact flash (CF) card.

Recommended Action: Check the availability and healthiness of the CF card immediately for proper functioning.

SLCD-1010

Message: `CF wear leveling daemon Failed to find any western digital (WD) CF cards attached.`

Message Type: LOG

Severity: ERROR

Probable Cause: Indicates an error in enumerating the attached compact flash (CF) cards.

Recommended Action: Check the availability and connection to the CF cards immediately for proper functioning.

SLCD-1011

Message: `CF life percentage used for card No. <CF Card number in integer> is <life span of CF used up in percentage>.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates the used life span of the compact flash (CF) card as reported by the CF wear leveling statistics.

Recommended Action: No action is required.

SNMP Messages

SNMP-1001

Message:`SNMP service is not available <Reason>.`

Message Type: LOG

Severity: ERROR

Probable Cause:

Indicates that the Simple Network Management Protocol (SNMP) service could not be started because of the specified reason. 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 using the **`show interface management`** command. If the specified reason is an initialization failure, reload the switch.

SNMP-1002

Message: `SNMP <Error Details> initialization failed.`

Message Type: LOG

Severity: ERROR

Probable Cause: Indicates that the initialization of the Simple Network Management Protocol (SNMP) service failed and you will not be able to query the switch through SNMP.

Recommended Action: Reload or power cycle the switch. This will automatically initialize SNMP.

SNMP-1003

Message: `Distribution of Community Strings to Secure Fabric failed.`

Message Type: LOG

Severity: ERROR

Probable Cause: Indicates that the changes in the Simple Network Management Protocol (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 using the **`snmp-server community`** command.

SNMP-1004

Message: `Incorrect SNMP configuration.`

Message Type: FFDC | LOG | AUDIT

Severity: ERROR

Probable Cause: Indicates that the Simple Network Management Protocol (SNMP) configuration is incorrect and the SNMP service will not work correctly.

Recommended Action: Change the SNMP configuration using the **`config snmp-server`** command.

SNMP-1005

Message: `SNMP configuration attribute, <Changed attribute>, <String Value>.`

Message Type: LOG | AUDIT

Class: CFG

Severity: INFO

Probable Cause: Indicates that the Simple Network Management Protocol (SNMP) configuration has changed. The parameter that was modified is displayed along with the old and new values of that parameter.

Recommended Action: Execute the **`show running-config snmp-server`** command to view the new SNMP configuration.

SRM Messages

SRM-1001

Message:`CPU usage reached <Percentage of current cpu usage> percent, exceeeded the threshold.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates the CPU usage exceeded the configured threshold, therefore triggered the alart action.

Recommended Action: Execute the **show process cpu** command for more information.

SRM-1002

Message:`The system free memory is at <current low memory usage> KBytes and is below the threshold.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates the system low memory usage exceeded the configured threshold.

Recommended Action: Execute the **show process memory** command for more information.

SRM-1003

Message:`High memory usage reached <current high memory usage> Kbytes, exeeceded the threshold.`

Message Type: LOG

Severity: WARNING

Probable Cause: Indicates the system high memory usage exceeded the configured threshold, therefore triggered the alart action.

Recommended Action: Execute the **show process memory** command for more information.

SRM-1004

Message:`Process <Process name and PID and current memory usage in KBytes> PID <Process name and PID and current memory usage in KBytes> memory usage reached <Process name and PID and current memory usage in KBytes> KBytes, exeeceded the alarm threshold.`

Message Type: LOG

Severity: WARNING

Probable Cause: Indicates the process based memory usage exceeded the configured alarm threshold, therefore triggered the alart action.

Recommended Action: Execute the **show process memory** command for more information. Check for memory leak if suspected.

SRM-1005

Message:`Process <Process name and PID and current memory usage in KBytes> PID <Process name and PID and current memory usage in KBytes> memory usage reached <Process name and PID and current memory usage in KBytes> KBytes, exceeded the critical threshold.`

Message Type: LOG

Severity: WARNING

Probable Cause: Indicates the process based memory usage exceeded the configured critical threshold, therefore triggered the alart action.

Recommended Action: Execute the **`show process memory`** command for more information.

SS Messages

SS-1000

Message: `Copy support upload operation is completed.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that the copy support command was used to transfer the support information to a remote location.

Recommended Action: No action is required.

SS-1001

Message:`Copy support upload operation has been aborted.`

Message Type: LOG

Severity: WARNING

Probable Cause: Indicates that a file copy error occurred during execution of the **`copy support`** command. Complete error information cannot always be displayed in this message because of possible errors in the subcommands being executed by the **`copy support`** command.

The file copy error can occur due to one of the following reasons:

• Could not connect to remote host

• Could not connect to remote host - timed out

• Transfer failed

- Transfer failed - timed out
- Directory change failed
- Directory change failed - timed out
- Malformed URL
- Usage error
- Error in login configuration file
- Session initialization failed
- Unknown remote host error

Recommended Action: Check and correct the remote server settings and configuration and then execute the copy support command again.

If the problem persists, contact your system administrator.

SS-1002

Message: `Copy support has stored support information to the USB storage device.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that the copy support command was used to transfer support information to an attached USB storage device.

Recommended Action: No action is required.

SS-1003

Message: `Copy support operation to USB storage device aborted.`

Message Type: LOG

Severity: WARNING

Probable Cause: Indicates that a USB operation error occurred during execution of the **`copy support`** command. Complete error information cannot always be displayed in this message because of possible errors in subcommands being executed by the **`copy support`** command.

Recommended Action: Make sure that the attached USB device is enabled.

Execute the usb on command to enable an attached USB device. After the USB problem is corrected, execute the **`copy support`** command again.

SS-1004

Message: `One or more modules timed out during copy support. Retry copy support with timeout option to collect all modules.`

Message Type: LOG

Severity: WARNING

Probable Cause: Indicates timeout in modules during execution of the **`copy support`** command.

Recommended Action: Execute the **`copy support`** command again.

SS-1010

Message: `Copy support timeout multiplier is set to <Timeout Multiplier> due to higher CPU load average. Copy support may take more time to complete.`

Message Type: LOG

Severity:INFO

Probable Cause: Indicates that the CPU load average is above normal. The copy support operation may take longer time than usual.

Recommended Action: No action is required.

SS-1011

Message: `Copy support upload operation failed. Reason: <Failure reason>.`

Message Type: LOG

Severity: WARNING

Probable Cause: Indicates that a file copy error occurred during execution of the **`copy support`** command.

The file copy error can occur due to one of the following reasons:

- Could not connect to remote host
- Could not connect to remote host - timed out
- Transfer failed
- Transfer failed - timed out
- Directory change failed
- Directory change failed - timed out

- Malformed URL
- Usage error
- Error in login configuration file
- Session initialization failed
- Unknown remote host error

Recommended Action: Check and correct the remote server settings and configuration and then execute the copy support command again.

If the problem persists, contact your system administrator.

SS-1012

Message: `Copy support upload Operation started.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that the copy support upload operation has started.

Recommended Action: No action is required.

SS-1013

Message: `Previous Copy support upload operation aborted abnormaly. If the issue persists, please run copy support protocol-type; group BASIC to capture the basic debugging information.`

Message Type: LOG | FFDC

Severity: WARNING

Probable Cause: Indicates that the copy support upload operation has aborted abnormaly.

Recommended Action: No action is required.

SS-1014

Message: `Insufficient physical memory(<Physical Memory free space > MB) for copy support.`

Message Type: LOG

Severity: WARNING

Probable Cause: Indicates that physical memory is below minimum requirement for copy support.

Recommended Action: No action is required.

SS-1015

Message: `Insufficient CF Memory(<CF free space > MB) for copy support.`

Message Type: LOG

Severity: WARNING

Probable Cause: Indicates that CF Memory is below minimum requirement for copy support.

Recommended Action: No action is required.

SS-1016

Message: `Copy support module <Module name>.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that the copy support operation has started on the specified module.

Recommended Action: No action is required.

SS-1017

Message: `Copy support group <Group name> could not be found.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that the copy support could not find the group name given by the user.

Recommended Action: No action is required.

SS-1018

Message: `Support files have been removed.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that the clear support removed core and ffdc files.

Recommended Action: No action is required.

SSMD Messages

SSMD-1001

Message:`Failed to allocate <Memory size> bytes of memory.`

Message Type: DCE

Severity: ERROR

Probable Cause: Indicates that the specified function has failed to allocate memory.

Recommended Action: Check the memory usage on the switch using the **`show process memory`** command.

Reload or power cycle the switch.

SSMD-1002

Message: `Failed to lock mutex.`

Message Type: DCE

Severity: ERROR

Probable Cause: Indicates that System Services Manager (SSM) component has failed to lock the mutex.

Recommended Action: Reload or power cycle the switch.

SSMD-1003

Message: `Failed to unlock mutex.`

Message Type: DCE

Severity: ERROR

Probable Cause: Indicates that System Services Manager (SSM) component has failed to unlock the mutex.

Recommended Action: Reload or power cycle the switch.

SSMD-1004

Message: `SSM startup failed.`

Message Type: DCE

Severity: ERROR

Probable Cause: Indicates that the Data Center Ethernet (DCE) System Services Manager (SSM) has encountered an unexpected severe error during basic startup and initialization.

Recommended Action: Reload or power cycle the switch.

If the problem persists, download a new firmware version using the **`firmware download`** command.

SSMD-1005

Message: <message>



Note
The message indicates that some packets are permitted/denied by ACL.

Message Type: DCE

Severity: INFO

Probable Cause: Acl logged packets

Recommended Action:ACL log feature enabled.

SSMD-1136

Message: `Ethertype Based VLAN Classifier Table is full on Chip <Slot Number>/<Slot Chip Number>:<Chip Core Number>.`

Message Type: DCE

Severity: ERROR

Probable Cause: Indicates that Ethertype-based VLAN classifier table is full.

Recommended Action: Clean up the unused Ethertype-based VLAN classifiers to add new ones.

SSMD-1236

Message: `MAC Based VLAN Classifier Table is full on Chip <Slot Number>/<Slot Chip Number>:<Chip Core Number>.`

Message Type: DCE

Severity: WARNING

Probable Cause: Indicates that MAC-based VLAN classifier table is full.

Recommended Action: Clean up the unused MAC-based VLAN classifiers to add new ones.

SSMD-1400

Message: `<ACL Type> access list <ACL Name> is created.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that the specified access list has been created.

Recommended Action: No action is required.

SSMD-1402

Message: `<ACL Type> access list <ACL Name> is deleted.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that the specified access list has been deleted.

Recommended Action: No action is required.

SSMD-1404

Message: `<ACL Type> access list <ACL Name> rule sequence number <rule_sq_no> is <action>.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that the access list rules are added to or removed from an existing policy.

Recommended Action: No action is required.

SSMD-1405

Message: `<ACL Type> access list <ACL Name> configured on interface <Interface Name> at <Direction> by <Configuration source>.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that the specified access list has been configured on the interface.

Recommended Action: No action is required.

SSMD-1406

Message: `<ACL Type> access list <ACL Name> is removed from interface <Interface Name> at <Direction> by <Configuration source>.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that the specified access list has been removed from the interface.

Recommended Action: No action is required.

SSMD-1407

Message: `<ACL Type> access list <ACL Name> active on interface <Interface Name> at <Direction>.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that the specified access list has been configured on the interface.

Recommended Action: No action is required.

SSMD-1408

Message: `<Number of ACL Rules> rules added to <ACL Type> access list <ACL Name>.`

Message Type: DCE

Severity:INFO

Probable Cause: Indicates that the specified rules are added to the access control list (ACL).

Recommended Action: No action is required.

SSMD-1409

Message: `Inbound ACL mirroring is active on interface <Source mirroring interface>`

Message Type: DCE

Severity:INFO

Probable Cause: Indicates that the access list mirroring is enabled.

Recommended Action: No action is required.

SSMD-1410

Message: `Inbound ACL mirroring is inactive on interface <Source mirroring interface>`

Message Type: DCE

Severity:INFO

Probable Cause: Indicates that the access list mirroring is disabled.

Recommended Action: No action is required.

SSMD-1411

Message: `<ACL Type> access list <ACL Name> configured on interface <InterfaceName> shall use interface associated vlan instead of vlan-id provided in rule config.`

Message Type: DCE

Severity:INFO

Probable Cause: Indicates that the interface will use interface associated vlan instead of vlan-id provided in rule config.

Recommended Action: No action is required.

SSMD-1412

Message: `MAC access list <ACL Name> configured on <VLAN Name> shall use vlan <VLAN Id> instead of vlan-id provided in rule config.`

Message Type: DCE

Severity:INFO

Probable Cause: Indicates that the interface will use vlan instead of vlan-id provided in rule config.

Recommended Action: No action is required.

SSMD-1413

Message: `<ACL Type> access list <ACL Name> resequence <action>.`

Message Type: DCE

Severity:INFO

Probable Cause: Indicates that the access list rules resequence command is success or failure

Recommended Action: No action is required.

SSMD-1436

Message: `<ACL Type> access list <ACL Name> partially active on interface <Interface Name> at <Direction>.`

Message Type: DCE

Severity:WARNING

Probable Cause: Indicates that the specified access control list (ACL) was not fully instantiated into the ternary content addressable memory (TCAM).

Recommended Action: Remove the specified ACL and other unused ACLs that are applied using the **`no ip access-groupname`**[**`in`**|**`out`**] command, and then instantiate ACL into TCAM again.

SSMD-1437

Message: `<ACL Type> access list <ACL Name> inactive on interface <Interface Name> at <Direction>.`

Message Type: DCE

Severity:WARNING

Probable Cause: Indicates the specified access control list (ACL) was not instantiated into the ternary content addressable memory (TCAM).

Recommended Action: Remove the specified ACL and other unused ACLs that are applied using the **`no ip access-groupname`**[**`in`**|**`out`**] command, and then instantiate ACL into TCAM again.

SSMD-1438

Message: `<ACL Type> access list <ACL Name> configured on interface <Interface Name> at <Direction> has rule(s) which are not supported on this platform.`

Message Type: DCE

Severity: WARNING

Probable Cause: Indicates that the specified access control list (ACL) has rules which are not supported on this platform.

Recommended Action: Remove unsupported rules using the **`no seq 0-4294967290`** command in the ACL context.

SSMD-1439

Message: `Rule with sequence number <ACL Rule Sequence number> of <ACL Type> access list <ACL Name> configured on interface <Interface Name> at <Direction> is not supported on this platform.`

Message Type: DCE

Severity:WARNING

Probable Cause: Indicates that the specified access control list (ACL) has rules which are not supported on this platform.

Recommended Action: Remove unsupported rules using the **`no seq 0-4294967290`** command in the ACL context.

SSMD-1440

Message: `<Warning string>`

Message Type: DCE

Severity:WARNING

Probable Cause: Indicates that the specified access control list (ACL) has rules which are not supported on this Tcam profile.

Recommended Action: Remove unsupported rules using the **`no seq 0-4294967290`** command in the ACL context.

SSMD-1498

Message: `ACL rules with <Feature Name> attributes are now <Feature Status>.`

Message Type: DCE

Severity:INFO

Probable Cause: Indicates that the duplicate/conflicting rules are now accepted/rejected by system.

Recommended Action: No action is required.

SSMD-1499

Message: `<Featurew Name> is now <Feature Status>.`

Message Type: DCE

Severity:INFO

Probable Cause: Indicates that acl-cam-sharing is enabled/disabled in the system.

Recommended Action: No action is required.

SSMD-1536

Message: `<Table Mode> <Feature Name> Table is full at <Table Type> on Chip <Slot Number>/<Slot Chip Number>:<Chip Core Number>.`

Message Type: DCE

Severity: WARNING

Probable Cause: Indicates that MAC-based VLAN classifier table is full.

Recommended Action: Clean up the unused MAC-based VLAN classifiers to add new ones.

SSMD-1571

Message: `Error <Error code> Creating region Feature:<Logical Device ID> Region:<Region ID> Chip:0x<Chip Index>.`

Message Type: DCE

Severity: ERROR

Probable Cause: Indicates that the application-specific integrated circuit (ASIC) driver has returned an error.

Recommended Action: Execute the **`copy support`** command and contact your switch service provider.

SSMD-1900

Message: `Security sub-profile is created for port-profile <Profile name>.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that a security sub-profile has been created for the specified port-profile.

Recommended Action: No action is required.

SSMD-1901

Message: `ACL <ACL name> is configured successfully for security sub-profile of port-profile <Profile name>.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that the specified access control list (ACL) has been configured for the security sub-profile.

Recommended Action: No action is required.

SSMD-1902

Message: `ACL <ACL name> is removed successfully for security sub-profile of port-profile <Profile name>.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that the specified access control list (ACL) has been removed for the security sub-profile.

Recommended Action: No action is required.

SSMD-1915

Message: `Security sub-profile is deleted for port-profile <Profile name>.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that the security sub-profile has been deleted.

Recommended Action: No action is required.

SULB Messages

SULB-1000

Message: `The firmware download command has been started.`

Message Type: AUDIT | LOG

Class: FIRMWARE

Severity: WARNING

Probable Cause: Indicates that firmware download has started.

Recommended Action: No action is required.

SULB-1100

Message:`Firmware <firmware operations: install, swap, reboot, commit, recover> begins on <slot/partition>.`

Message Type:AUDIT | LOG

Class: FIRMWARE

Severity: INFO

Probable Cause: Indicates that the specified firmware operation has started on the specified slot or partition.

Recommended Action: No action is required.

SULB-1101

Message: `Firmware <firmware operations: install, swap, reboot, commit, recover> ends on <slot/partition>.`

Message Type: AUDIT | LOG

Class: FIRMWARE

Severity: INFO

Probable Cause: Indicates that the specified firmware operation has completed successfully on the specified slot or partition.

Recommended Action: No action is required.

SULB-1102

Message: `Firmware <firmware operations: install, swap, reboot, commit, recover> failed on <slot/partition> with error (<error code>).`

Message Type: AUDIT | LOG

Class: FIRMWARE

Severity: WARNING

Probable Cause: Indicates that specified firmware operation has failed on the specified slot or partition. The error code indicates the reason for the failure.

The following table lists the error codes that provide more details on why the firmware operation failed.

Error message	Error code
"Upgrade is inconsistent."	0x10
"OSRootPartition is inconsistent."	0x11

Error message	Error code
"Unable to access the package list file. Check whether the file name is specified properly."	0x12
"Red Hat package manager (RPM) package database is inconsistent. Contact your service provider for recovery."	0x13
"Out of memory."	0x14
"Failed to download RPM package. Check if the firmware image is accessible."	0x15
"Unable to create firmware version file."	0x16
"Unexpected system error."	0x17
"Another firmware download is in progress."	0x18
"Error in releasing lock device."	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. Contact your service provider to assistance."	0x1c
"OSLoader is inconsistent.	0x1d
"New image has not been committed. Execute the **`firmware commit`** command or the **`firmware restore`** and **`firmware download`** commands."	0x1e
"**`firmware restore`** is not needed."	0x1f
"Images are not mounted properly."	0x20
"Unable to uninstall old packages. Contact your service provider for assistance."	0x21
"**`firmware download`** has timed out."	0x23
"Out of disk space."	0x24
"Primary filesystem is inconsistent. Execute the **`firmware restore`** to restore the original firmware, or contact your service provider for recovery."	0x25
"The post-install script failed."	0x26
"Reload (partition) failed."	0x27
"Primary kernel partition is inconsistent. Contact your service provider for recovery."	0x28
"The pre-install script failed."	0x29
"Failed to install RPM package."	0x2b
"Cannot downgrade directly to this version. Downgrade to an intermediate version and then download the desired version."	0x2c
"Failed to validate firmware signature."	0x3e

Error message	Error code
"Failed to swap the firmware partitions."	0x40
"Failed to load the PROM image. Contact your service provider for assistance."	0x41

Recommended Action: Execute the **`show firmwaredownloadstatus`** command for more information. Restart the firmware operation if needed.

SULB-1103

Message:`Firmware download completed successfully on <slot/partition>.`

Message Type:AUDIT | LOG

Class: FIRMWARE

Severity: INFO

Probable Cause: Indicates that the specified firmware download has completed successfully on the specified slot or partition.

Recommended Action: No action is required.

Execute the **`show firmwaredownloadstatus`** command for more information. Execute the **`show version`** to verify the firmware version.

SULB-1104

Message: `Firmware download <failed or failed but recovered> on <node name> with error (<error code>).`

Message Type: AUDIT | LOG

Class: FIRMWARE

Severity: CRITICAL

Probable Cause: Indicates that firmware download has failed on the specified slot. The error code indicates the reason for the failure.

The following table lists the error codes that provide more details on why the firmware operation failed.

Error message	Error code
"No error."	0x0
"Upgrade is inconsistent."	0x10
"OSRootPartition is inconsistent."	0x11

Error message	Error code
"Unable to access the package list file. Check whether the file name is specified properly."	0x12
"Red Hat package manager (RPM) package database is inconsistent. Contact your service provider for recovery."	0x13
"Out of memory."	0x14
"Failed to download RPM package. Check if the firmware image is accessible."	0x15
"Unable to create firmware version file."	0x16
"Unexpected system error."	0x17
"Another firmware download is in progress."	0x18
"Error in releasing lock device."	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. Contact your service provider to assistance."	0x1c
"OSLoader is inconsistent.	0x1d
"New image has not been committed. Execute the **`firmware commit`** command or the **`firmware restore`** and **`firmware download`** commands."	0x1e
"**`firmware restore`** is not needed."	0x1f
"Images are not mounted properly."	0x20
"Unable to uninstall old packages. Contact your service provider for assistance."	0x21
"**`firmware download`** has timed out."	0x23
"Out of disk space."	0x24
"Primary filesystem is inconsistent. Execute the **`firmware restore`** to restore the original firmware, or contact your service provider for recovery."	0x25
"The post-install script failed."	0x26
"Reload (partition) failed."	0x27
"Primary kernel partition is inconsistent. Contact your service provider for recovery."	0x28
"The pre-install script failed."	0x29
"Failed to install RPM package."	0x2b
"Cannot downgrade directly to this version. Downgrade to an intermediate version and then download the desired version."	0x2c
"Failed to validate firmware signature."	0x3e

Error message	Error code
"Failed to swap the firmware partitions."	0x40
"Failed to load the PROM image. Contact your service provider for assistance."	0x41

Recommended Action: Execute the **`show firmwaredownloadstatus`** command for more information. Execute the **`power-off`** and **`power-on`** commands on the slot for recovery.

SULB-1105

Message: `Firmware upgrade session (<session ID>: <session subject>) starts.`

Message Type: AUDIT | LOG

Class: FIRMWARE

Severity: WARNING

Probable Cause: Indicates that firmware upgrade has started.

Recommended Action: No action is required.

SULB-1106

Message: `Firmware upgrade session (<session ID>: <session subject>) completes.`

Message Type: AUDIT | LOG

Class: FIRMWARE

Severity: WARNING

Probable Cause: Indicates that firmware upgrade has completed successfully.

Recommended Action: Execute the **`show firmwaredownloadstatus`** command for more information.

SULB-1107

Message: `Firmware upgrade session (<session ID>: <session subject>) failed but recovered.`

Message Type: LOG

Class: FIRMWARE

Severity: WARNING

Probable Cause: Indicates that firmware upgrade has failed but was recovered.

Recommended Action: Execute the **`show firmwaredownloadstatus`** command for more information.

Execute the **`firmware download`** command again if needed.

SULB-1108

Message: `Firmware upgrade session (<session ID>: <session subject>) failed.`

Message Type: LOG

Class: FIRMWARE

Severity: CRITICAL

Probable Cause: Indicates that firmware upgrade has failed.

Recommended Action: Execute the **`show firmwaredownloadstatus`** command for more information.

Execute the **`firmware download`** command again if needed.

SULB-1109

Message: `Firmware upgrade session (<session ID>: <session subject>) aborted.`

Message Type: LOG

Class: FIRMWARE

Severity: CRITICAL

Probable Cause: Indicates that firmware upgrade has been aborted.

Recommended Action:

Execute the **`firmware download`** command again if needed.

SULB-1110

Message: `Firmware upgrade session (<session ID>: <session subject>) has completed the installation successfully.`

Message Type: LOG

Class: FIRMWARE

Severity: WARNING

Probable Cause: Indicates that firmware upgrade has completed.

Recommended Action: No action is required.

SULB-1211

Message: `<device-detail>, [slxCoreHndlr] coredump started for process {pid:<process-id> epoc timestamp:<timestamp> comm:<command> cmdline:<executed-command-line> file:<core-file-with-path>`

Message Type: LOG

Class: FIRMWARE

Severity: INFO

Probable Cause: Start of coredump.

The following table lists the fields in the error messages.

Table 13: Fields and Description

Field	Description
<device-id>	The device name on which the crash file was generated.
pid <process-id>	The process ID of the process which crashed and generated the coredump file.
epoc timestamp <timestamp>	The timestamp when the coredump file was started.
comm <command>	The command which generated the coredump.
cmdline <executed-command-line>	The complete command that was executed.
file <core-file-with-path>	The complete path to the coredump file.

SULB-1212

Message: `<device-detail>, [slxCoreHndlr] coredump completed for process {pid:<process-id> epoc timestamp:<timestamp> file:<core-file-with-path> (size:<file-size-in-bytes>)`

Message Type: LOG

Class: FIRMWARE

Severity: INFO

Probable Cause: Successful completion of coredump.

For more information on the fields in this error message, see table Table 13 on page 408

SULB-1213

Message: `<device-detail>, [slxCoreHndlr] ERROR: Failed to save core dump to <core-file-with-path>`

Message Type: LOG

Class: FIRMWARE

Severity: ERROR

Probable Cause: Core file not saved to disk.

For more information on the fields in this error message, see table Table 13 on page 408

SULB-1214

Message: `<device-detail>, [slxCoreHndlr] ERROR: Failed to compress. Core dump saved to <core-file-with-path>`

Message Type: LOG

Class: FIRMWARE

Severity: ERROR

Probable Cause: Failed to compress the corefile before saving to disk.

For more information on the fields in this error message, see table Table 13 on page 408

SWCH 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

Severity: ERROR

Probable Cause: Indicates failure to enable the switch because it is not in the ready state.

Recommended Action: If the message persists, execute the copy support 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

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 **`show secpolicy`** command to verify whether the specified device World Wide Name (WWN) is listed. If it is not listed, execute the **`secpolicy defined-policy`** command to add this device to an existing policy.

SWCH-1004

Message: `Interface module attach failed during recovery, disabling slot = <slot number>.`

Message Type: LOG

Severity: ERROR

Probable Cause: Indicates that the specified interface module has failed during or recovery.

Recommended Action: For a modular switch, execute the **`power-off`** and **`power-on`** commands to power cycle the interface module.

For a compact switch, reload or power cycle the switch.

SWCH-1005

Message: `Diag attach failed during recovery, disabling slot = <slot number>.`

Message Type: LOG

Severity: ERROR

Probable Cause: Indicates that the diagnostic interface module attach operation has failed during or recovery.

Recommended Action: For a modular switch, execute the **`power-off`** and **`power-on`** commands to power cycle the interface module.

For a compact switch, reload or power cycle the switch.

SWCH-1007

Message: `Switch port <port number> disabled due to \"<disable reason>\".`

Message Type: LOG

Severity: WARNING

Probable Cause: Indicates that the specified switch port is disabled due to the reason displayed in the message.

Recommended Action: Take corrective action to restore the port based on the disable reason displayed in the message and then execute the **shutdown** and **no shutdown** commands.

SWCH-1021

Message: `HA state out of sync: Standby MM (ver = <standby SWC version>) does not support Dynamic area on default switch (Active MM version = <active SWC version>).`

Message Type: LOG

Severity: WARNING

Probable Cause: Indicates that the standby management module does not support the dynamic area on the default switch.

Recommended Action: Load a firmware version in which the standby management module supports the dynamic area on the default switch using the **firmware download** command.

SWCH-1023

Message: `HA state out of sync: Standby MM (ver = <standby SWC version>) does not support active's enforce_login policy (Active MM version =<active SWC version>).`

Message Type: LOG

Severity: WARNING

Probable Cause: Indicates that the standby management module does not enforce login policy of the active management module.

Recommended Action: Configure the enforce login policy to a value that the standby management module supports.

SWCH-1024

Message: `Rebooting the standby, received a duplicate update for port [<Port Number>]`

Message Type: LOG | FFDC

Severity: INFO

Probable Cause: Indicates that the standby CP received duplicate port create event for a port which is probably due to LC coming online while syncing the backup MM. The standby CP reboots automatically to ensure sync and attain normal state. This is a rare occurrence.

Recommended Action: No Action is required.

TNDL Messages

TNDL-1000

Message: `TunnelMgr initialized successfully.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that the Data Center Ethernet (DCE) tunnel manager has been initialized.

Recommended Action: None

TNDL-1001

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

Message Type: LOG

Severity: ERROR

Probable Cause: Indicates that the specified function has failed to allocate memory.

Recommended Action: Check the memory usage on the switch using the **`show process memory`** command.

Restart or power cycle the switch.

TNDL-1005

Message: `TunnelMgr startup failed.`

Message Type: LOG

Severity: ERROR

Probable Cause: Indicates that the Data Center Ethernet (DCE) tunnel manager encountered an unexpected severe error during basic startup and initialization.

Recommended Action: Restart or power cycle the switch.

If the problem persists, download a new firmware version using the **`firmware download`** command.

TNDL-1006

Message: `Tunnel <tunnel ID> creation failed.`

Message Type: LOG

Severity: ERROR

Probable Cause: Indicates that the tunnel creation was unsuccessful.

Recommended Action: Technical support is required.

TNDL-1007

Message: `Tunnel <tunnel ID> deletion failed.`

Message Type: LOG

Severity: ERROR

Probable Cause: Indicates that the tunnel deletion was unsuccessful.

Recommended Action: Technical support is required.

TNDL-2001

Message: `NSX controller pushed more than <Safe Ucast_Macs_Remote limit> Ucast_Macs_Remote objects. This may result in unexpected traffic behavior.`

Message Type: LOG

Severity: WARNING

Probable Cause: Indicates that the switch may be connecting to NSX controllers having huge number of configurations which are beyond scale capacity of the switch. There could be traffic loss or unexpected behavior.

Recommended Action: Update configurations in NSX controller accordingly.

TNDL-2011

Message: `Delete duplicate Mcast_Macs_Remote entry; MAC=\"<Multicast MAC>\", logical_switch=\"<Logical_Switch name>\".`

Message Type: LOG

Severity: ERROR

Probable Cause: Indicates an unexpected error while communicating to the VMware NSX controller.

Recommended Action: Undo all operations and try again.

TNDL-2012

Message: `Local MAC \"<MAC address>\" already exists in Ucast_Macs_Remote table; skipping write to Ucast_Macs_Local.`

Message Type: LOG

Severity: ERROR

Probable Cause: Indicates that Layer 2 system (L2SYS) has notified a MAC entry that was learned from the VMware NSX controller.

Recommended Action: Undo all operations and try again.

TNDL-2013

Message: `Failed to cleanup Overlay Gateway Configuration during reconcile.`

Message Type: LOG

Severity: ERROR

Probable Cause: Indicates that cleanup of tunnels or local MAC entries has failed in the back-end.

Recommended Action: Undo all operations and try again.

TNDL-2014

Message: `Tunnel id conflict detected for one or more tunnels. Automatic recovery initiated.`

Message Type: LOG

Severity: ERROR

Probable Cause: Indicates that tunnel ID conflict is detected for one or more tunnels.

Recommended Action: The system initiates automatic recovery.

TNDL-2015

Message: `Tunnel creation failed (source <> destination <>) due to max number of tunnels reached(<>).`

Message Type: LOG

Severity: ERROR

Probable Cause: Indicates that tunnel creation failed as max supported number of tunnels reached.

Recommended Action: Delete some other tunnels and retry.

TNLD-2016

Message: `Tunnel resource has reached user configured high threshold limit.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that the number of active tunnels has crossed the user configured high threshold level.

Recommended Action: Close some active tunnels.

TNDL-2017

Message: `Tunnel resource dropped below user configured low threshold limit.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that the number of active tunnels has dropped below the user configured low threshold level.

Recommended Action: No action is required.

TOAM Messages

TOAM-1003

Message:`Initilization error: <reason>.`

Message Type: DCE

Severity: ERROR

Probable Cause: Indicates that TRILL OAM (TOAM) has encountered an error during initialization.

Recommended Action: Reload or power cycle the switch.

TRCE Messages

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

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.

Recommended Action: No action is required.

TRCE-1003

Message:`Trace dump<optional slot indicating on which slot the dump occurs> was not transferred due to FTP error.`

Message Type: LOG

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: If the message persists, execute the **`copy support`** command and contact your switch service provider.

TRCE-1005

Message: `FTP Connectivity Test failed due to error.`

Message Type: LOG

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 **`copy support`** 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

Severity: INFO

Probable Cause: Indicates that a connectivity test to the FTP host has succeeded.

Recommended Action: No action is required.

TRCE-1007

Message: `Notification of this MM has failed. Parameters temporarily out of sync with other MM.`

Message Type: LOG

Severity: ERROR

Probable Cause: Indicates that the active management module was unable to alert the standby management module of a change in the trace status. This message is only applicable to modular switches

Recommended Action: This message is often transitory. Wait a few minutes and try the command again.

If the message persists, execute the **`copy support`** command and contact your switch service provider.

TRCE-1008

Message: `Unable to load trace parameters.`

Message Type: FFDC | LOG

Severity: CRITICAL

Probable Cause: Indicates that the management module is unable to read the stored trace parameters.

Recommended Action: Reload the switch or the chassis.

If the message persists, execute the **`copy support`** command and contact your switch service provider.

TRCE-1009

Message: `Unable to alert active MM that a dump has occurred.`

Message Type: LOG

Severity: WARNING

Probable Cause: Indicates that the standby management module is unable to communicate trace information to the active management module. This message is only applicable to modular switches.

Recommended Action: Execute the show ha command to verify that the current management module is standby and the active management module is active.

If the message persists, execute the **`copy support`** command and contact your switch service provider.

TRCE-1010

Message: `Traced fails to start.`

Message Type: LOG

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: If the message persists, reload the switch or the chassis.

Execute the **`copy support`** 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

Severity:INFO

Probable Cause: Indicates that the trace dump files were transferred manually to the specified slot.

Recommended Action: No action is required.

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

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 **`copy support`** command and contact your switch service provider.

TS Messages

TS-1001

Message: `NTP query to configured external clock servers(s) failed. Local clock time will be used.`

Message Type: LOG

Severity: WARNING

Probable Cause: Indicates a network time protocol (NTP) query to the configured external clock server failed. When next server is not configured local clock time is used for synchronization. This might be logged during temporary operational issues such as IP network connection issues to the external clock server. If it does not recur, it can be ignored.

Recommended Action: Verify the configured external clock server is available and functional. If that external clock server is not available, choose another.

TS-1002

Message: `<Type of clock server used> Clock Server 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

Severity: INFO

Probable Cause: Indicates that the switch 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 switch clock.

• 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. If the message does not recur, it can be ignored.

Recommended Action: Execute the **`show ntp status`** command to verify that the switch clock server IP address is configured correctly.

Verify if this clock server is accessible to the switch and functional. If it is not accessible or functional, configure an accessible and functional clock server or reset the clock server to local clock server (LOCL).

TS-1008

Message: `<New clock server used> Clock Server used instead of <Old server configured>. System time changed from <Old time> to <New time>.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that the source of switch time synchronization was changed to another configured clock server because the Network Time Protocol (NTP) query to the current active external clock server failed.

Recommended Action: No action is required. New clock server synchronization will adjust the clock time.

TS-1009

Message:`Event: change time: attempt.`

Message Type: AUDIT

Class: SECURITY

Severity: INFO

Probable Cause: Indicates an attempt to change the switch time.

Recommended Action: No action is required.

TS-1010

Message: `Event: change time: <success or fail>, Info: <result detail>.`

Message Type: AUDIT

Class: SECURITY

Severity: INFO

Probable Cause: Indicates the status of the switch time change.

Recommended Action: No action is required.

TS-1011

Message: `Event: change time zone: attempt.`

Message Type: AUDIT

Class: SECURITY

Severity: INFO

Probable Cause: Indicates an attempt to change the time zone.

Recommended Action: No action is required.

TS-1012

Message: `Event: change time zone: <success or fail>, Info: <result detail>.`

Message Type: AUDIT

Class: SECURITY

Severity: INFO

Probable Cause: Indicates the status of the time zone change.

Recommended Action: No action is required.

TS-1013

Message: `Event: Clock Server change, Status: success, Info: <New clock server used> Clock Server used instead of <Old server configured>. System time changed from <Old time> to <New time>.`

Message Type: AUDIT

Class: SECURITY

Severity: INFO

Probable Cause: Indicates that the clock server and the system time have been changed.

Recommended Action: No action is required.

UCST Messages

UDLD Messages

UDLD-1000

Message: `UDLD is enabled.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that the UniDirectional Link Detection (UDLD) protocol is enabled globally.

Recommended Action: No action is required.

UDLD-1001

Message:`UDLD is disabled.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that the UniDirectional Link Detection (UDLD) protocol is disabled globally.

Recommended Action: No action is required.

UDLD-1002

Message: `UDLD Hello time has changed.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that the UniDirectional Link Detection (UDLD) Hello time has been changed.

Recommended Action: No action is required.

UDLD-1003

Message: `UDLD Multiplier timeout has changed.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that the UniDirectional Link Detection (UDLD) timeout multiplier value has been changed.

Recommended Action: No action is required.

UDLD-1004

Message: `UDLD is enabled on interface <InterfaceName>.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that the UniDirectional Link Detection (UDLD) protocol is enabled on the specified interface.

Recommended Action: No action is required.

UDLD-1005

Message: `UDLD is disabled on interface <InterfaceName>.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that the UniDirectional Link Detection (UDLD) protocol is disabled on the specified interface.

Recommended Action: No action is required.

UDLD-1006

Message: `Link status on interface <InterfaceName> is down. Unidirectional link detected.`

Message Type: LOG

Severity: ERROR

Probable Cause: Indicates that the specified interface has been detected as a unidirectional link. The interface is blocked.

Recommended Action: Action must be taken to fix the unidirectional link.

UDLD-1007

Message: `Link status on interface <InterfaceName> is up. Bidirectional link detected.`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that UniDirectional Link Detection (UDLD) PDUs are being received on a link that was considered unidirectional.

Recommended Action: No action is required.

UPTH Messages

UPTH-1001

Message: `No minimum cost path in candidate list.`

Message Type: LOG

Severity: WARNING

Probable Cause: Indicates that the switch is unreachable because no minimum cost path (MPATH) exists in the candidate list .

Recommended Action: No action is required. This error will end the current shortest path first (SPF) computation.

VRRP Messages

VRRP-1001

Message:`%s: Indicates that the system has failed to allocate memory%s.`

Message Type: DCE

Severity: ERROR

Probable Cause: Indicates that the system has failed to allocate memory.

Recommended Action: Check the memory usage on the switch using the show process memory command.

Reload or power cycle the switch.

VRRP-1002

Message: `VRRP%s %s [Session %d] state changed from Init To Master, Reason: Session is the owner.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that the Virtual Router Redundancy Protocol (VRRP) session state has changed.

Recommended Action: No action required.

VRRP-1003

Message: `VRRP%s %s [Session %d] state changed from Init To Backup, Reason: Session is not the owner.`

Message Type: DCE

Severity: INFO

Probable Cause: Indicates that the Virtual Router Redundancy Protocol (VRRP) session is enabled.

Recommended Action: No action required.

VRRP-1004

Message: `VRRP%s %s [Session %d] state changed from Backup To Master, Reason: Hold timer and Session timer expired`

Message Type:LOG | DCE

Severity: INFO

Probable Cause: Indicates that the Virtual Router Redundancy Protocol (VRRP) session state transition from Backup to Master.

Recommended Action: No action required.

VRRP-1005

Message: `VRRP%s %s [Session %d] state changed from Backup To Master, Reason: Hold timer and Session timer expired.`

Message Type:LOG | DCE

Severity: INFO

Probable Cause: Indicates that the Virtual Router Redundancy Protocol (VRRP) session state transition from Backup to Master.

Recommended Action: No action required.

VRRP-1006

Message: `VRRP%s %s [Session %d] state changed from Backup To Master, Reason: Neighbor Interface IP is lower.`

Message Type:LOG | DCE

Severity: INFO

Probable Cause: Indicates that the Virtual Router Redundancy Protocol/ (VRRP) session state transition from Backup to Master.

Recommended Action: No action required.

VRRP-1007

Message: `VRRP%s %s [Session %d] state changed from Master To Backup, Reason: Neighbor priority is higher.`

Message Type:LOG | DCE

Severity: INFO

Probable Cause: Indicates that the Virtual Router Redundancy Protocol (VRRP) session state transition from Master to Backup.

Recommended Action: No action required.

VRRP-1008

Message: `VRRP%s %s [Session %d] state changed from Master To Backup, Reason: Neighbor Interface IP is higher.`

Message Type:LOG | DCE

Severity: INFO

Probable Cause: Indicates that the Virtual Router Redundancy Protocol (VRRP) session state transition from Master to Backup.

Recommended Action: No action required.

VRRP-1009

Message: `VRRP%s %s Session %d is enabled.`

Message Type:LOG | DCE

Severity: INFO

Probable Cause: Indicates that the Virtual Router Redundancy Protocol (VRRP) session is enabled.

Recommended Action: No action required.

VRRP-1010

Message: `VRRP%s %s Session %d is disabled.`

Message Type:LOG | DCE

Severity: INFO

Probable Cause: Indicates that the Virtual Router Redundancy Protocol (VRRP) session is disabled.

Recommended Action: No action required.

VRRP-1501

Message: `%s:Unexpected error on deleting VRRP session.`

Message Type: LOG | DCE

Severity: ERROR

Probable Cause: Indicates that the system has failed to initialize.

Recommended Action: Reload or power cycle the switch.

VRRP-1502

Message: `Unexpected error deleting Anycast-Gateway IPv6 session.`

Message Type: LOG | DCE

Severity: ERROR

Probable Cause: Indicates that the system has failed to deleting Anycast-Gateway IPv6 session.

Recommended Action: Reload or power cycle the switch.

VRRP-1503

Message: `Unable to allocate message queue.`

Message Type: LOG | DCE

Severity: ERROR

Probable Cause: Indicates that the system has failed to allocate message queue.

Recommended Action: Reload or power cycle the switch.

VRRP-1504

Message: `ASP/IOT initialization failed.`

Message Type: LOG | DCE

Severity: ERROR

Probable Cause: Indicates that the system has failed to initilize ASP/IOT.

Recommended Action: Reload or power cycle the switch.

VRRP-1505

Message: `FSS registration error.`

Message Type: LOG | DCE

Severity: ERROR

Probable Cause: Indicates that the system has failed to register fss.

Recommended Action: Reload or power cycle the switch.

VRRP-1506

Message: `Could not open the version file to read.`

Message Type: LOG | DCE

Severity: ERROR

Probable Cause: Indicates that the system has failed to open the version file.

Recommended Action: Reload or power cycle the switch.

VRRP-1507

Message: `Cannot create <Table_name> during initialization of VR.`

Message Type: LOG | DCE

Severity: ERROR

Probable Cause: Indicates that the system has failed to create Association or Session table.

Recommended Action: Reload or power cycle the switch.

VRRP-1508

Message: `Unexpected error on disabling VRRP session.`

Message Type: LOG | DCE

Severity: ERROR

Probable Cause: Indicates the Unexpected error during VRRP Session disable.

Recommended Action: Reload or power cycle the switch.

VRRP-1509

Message: `NSM server protocol version error.`

Message Type: LOG | DCE

Severity: ERROR

Probable Cause: Indicates the NSM Server Protocol Version Error.

Recommended Action: Reload or power cycle the switch.

VRRP-1510

Message: `NSM service is not sufficient.`

Message Type: LOG | DCE

Severity: ERROR

Probable Cause: Indicates the NSM Service is not sufficient.

Recommended Action: Reload or power cycle the switch.

VRRP-1511

Message: `VRRP HA Registration failed.`

Message Type: LOG | DCE

Severity: ERROR

Probable Cause: Indicates the VRRP HA Registration Failure.

Recommended Action: Reload or power cycle the switch.

VRRP-1512

Message: `VRRP HA Configuration failed.`

Message Type: LOG | DCE

Severity: ERROR

Probable Cause: Indicates the VRRP HA Configuration Failure.

Recommended Action: Reload or power cycle the switch.

VRRP-1513

Message: `Fail to INIT NSM THA Library.`

Message Type: LOG | DCE

Severity: ERROR

Probable Cause: Indicates the VRRP NSM HA Initilization Failure.

Recommended Action: Reload or power cycle the switch.

VRRP-1514

Message: `nsm_lib_ha_tp_register failed.`

Message Type: LOG | DCE

Severity: ERROR

Probable Cause: Indicates the VRRP NSM Library Registration Failure.

Recommended Action: Reload or power cycle the switch.

VRRP-1515

Message: `VRRP HA deregister failed.`

Message Type: LOG | DCE

Severity: ERROR

Probable Cause: Indicates the VRRP deregister Failure.

Recommended Action: Reload or power cycle the switch.

VRRP-1516

Message: `Could not read the revision from the file.`

Message Type: LOG | DCE

Severity: ERROR

Probable Cause: Indicates that the system has failed to read revision from the file.

Recommended Action: Reload or power cycle the switch.

VRRP-2001

Message: `Error opening Socket.`

Message Type: LOG | DCE

Severity: ERROR

Probable Cause: Indicates VRRP Error in Opening the socket.

Recommended Action: If this is a modular switch, execute the command. If the problem persists or if this is a compact switch, download a new firmware version using the **`firmware download`** command.

VRRP-2002

Message: `IP_ADD_MEMBERSHIP to <Membership_name> failed. Membership already exists.`

Message Type: LOG | DCE

Severity: ERROR

Probable Cause: Indicates VRRP Error in the IP Add Membership.

Recommended Action:

VRRP-2003

Message: `Could not set IP_ADD_MEMBERSHIP option on the socket.`

Message Type: LOG | DCE

Severity: ERROR

Probable Cause: Indicates VRRP Error in the IP Add Membership option.

Recommended Action:

VRRP-2004

Message: `IP_DROP_MEMBERSHIP to <Membership_name> membership doesn't exist.`

Message Type: LOG | DCE

Severity: ERROR

Probable Cause: Indicates VRRP Error in the IP DROP Membership.

Recommended Action:

VRRP-2005

Message: `Can't setsockopt IP_DROP_MEMBERSHIP:`

Message Type: LOG | DCE

Severity: ERROR

Probable Cause: Indicates VRRP setsockopt Error in setting IP DROP Membership.

Recommended Action:

VRRP-2006

Message: `Socket creation failed.`

Message Type: LOG | DCE

Severity: ERROR

Probable Cause: Indicates VRRP Socket creation error.

Recommended Action:

VRRP-2007

Message: `Setting <Multicast_Type> Multicast hops failed:`

Message Type: LOG | DCE

Severity: ERROR

Probable Cause: Indicates VRRP Error in Setting IPv4 Multihop.

Recommended Action:

VRRP-2008

Message: `Failed to enable recv all VRF on socket.Error:`

Message Type: LOG | DCE

Severity: ERROR

Probable Cause: Indicates VRRP Socket enable recv error.

Recommended Action:

VRRP-2009

Message: `Setting IPv4 TOS precedence failed:`

Message Type: LOG | DCE

Severity: ERROR

Probable Cause: Indicates VRRP Error in setting TOS Precedence.

Recommended Action:

VRRP-2010

Message: `Setting recvif socket option on failed:`

Message Type: LOG | DCE

Severity: ERROR

Probable Cause: Indicates VRRP Error in setting recvif socket option.

Recommended Action:

VRRP-2011

Message: `Failed to disable loopback on socket.Error:`

Message Type: LOG | DCE

Severity: ERROR

Probable Cause: Indicates VRRP Error in disabling Loopback port.

Recommended Action:

VRRP-2012

Message: `Cannot set socket option to receive destination address.`

Message Type: LOG | DCE

Severity: ERROR

Probable Cause: Indicates VRRP Socket Error in setting destination Address.

Recommended Action:

VRRP-2013

Message: `OS Can't bind VRRP socket:`

Message Type: LOG | DCE

Severity: ERROR

Probable Cause: Indicates VRRP Error in bind socket.

Recommended Action:

VRRP-2014

Message: `Setting SO_REUSEADDR failed:`

Message Type: LOG | DCE

Severity: ERROR

Probable Cause: Indicates VRRP Reuse Address Error.

Recommended Action:

VRRP-2015

Message: `Cannot set hoplimit:`

Message Type: LOG | DCE

Severity: ERROR

Probable Cause: Indicates VRRP Error in Setting hoplimit.

Recommended Action:

VRRP-2016

Message: `Cannot Set Traffic Class:`

Message Type: LOG | DCE

Severity: ERROR

Probable Cause: Indicates VRRP Error in Setting Traffic Class.

Recommended Action:

VRRP-2017

Message: `Error transmitting VRRP advertisement.`

Message Type: LOG | DCE

Severity: ERROR

Probable Cause: Indicates VRRP Error in Sending Advertisement.

Recommended Action:

VRRP-2018

Message: `Setting ipv6 set failed.`

Message Type: LOG | DCE

Severity: ERROR

Probable Cause: Indicates VRRP Socket set option Error.

Recommended Action:

VRRP-2019

Message: `Cannot set IPv6 Checksum.`

Message Type:LOG | DCE

Severity: ERROR

Probable Cause: Indicates VRRP IPv6 Set CheckSum Error.

Recommended Action:

VRRP-2020

Message: `NL Socket creation failed group: <group_name>`

Message Type: LOG | DCE

Severity: ERROR

Probable Cause: Indicates VRRP Group Socket Creation Error.

Recommended Action:

VRRP-2021

Message: `NL Socket %s buffer size set failed for Socket: %d Group: %d.`

Message Type: LOG | DCE

Severity: ERROR

Probable Cause: Indicates VRRP Group Error in setting socked Send/Recv Buffer.

Recommended Action:

VRRP-2022

Message: `Failed to bind nl socket.`

Message Type: LOG | DCE

Severity: ERROR

Probable Cause: Indicates VRRP Bind Error.

Recommended Action:

VRRP-2023

Message: `Failed to Set setsockopt for group VRRP_GROUP_EVENT:<Event_Id>.`

Message Type: LOG | DCE

Severity: ERROR

Probable Cause: Indicates VRRP Group Error in setsockopt.

Recommended Action:

VRRP-5001

Message: `The input parameter is invalid.`

Message Type: LOG | DCE

Severity: ERROR

Probable Cause: The input parameter is invalid.

Recommended Action: Make sure to input or pass the right parameter from cli or other daemon.

VRRP-5201

Message: `Error in Transmitting Gratuitous ARP or ND.`

Message Type: LOG | DCE

Severity: ERROR

Probable Cause: Error in Sending Gratuitous ARP or ND.

Recommended Action:

VRRP-5301

Message: `FE State change failed for AF %d Session %d Interface.`

Message Type: LOG | DCE

Severity: ERROR

Probable Cause: VRRP State Chage Error.

Recommended Action:

VRRP-5302

Message: `add/delete Failed. Error Code <Error_code>`

Message Type: LOG | DCE

Severity: ERROR

Probable Cause: VRRP VMAC VIP Addition/Deletion Error.

Recommended Action:

VRRP-5303

Message: `Error leaving mcast group.`

Message Type: LOG | DCE

Severity: ERROR

Probable Cause: VRRP mcast group Error.

Recommended Action:

VRRP-5304

Message: `State change to Master for AF <Session_id> Interface <Interface_Id> Failed.`

Message Type: LOG | DCE

Severity: ERROR

Probable Cause: VRRP State Chage Error.

Recommended Action:

WEBD Messages

WEBD-1001

Message:`Missing or Invalid Certificate file -- HTTPS is configured but could not be started.`

Message Type: LOG

Severity: WARNING

Probable Cause: Indicates the SSL certificate file is either invalid or absent.

Recommended Action: Install a valid key file.

WEBD-1002

Message: `Missing or Invalid Key file -- HTTPS is configured but could not be started.`

Message Type: LOG

Severity: WARNING

Probable Cause: Indicates the 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

Severity: INFO

Probable Cause: Indicates the HTTP server configuration has changed.

Recommended Action: No action is required.

WEBD-1005

Message: `HTTP server and weblinker process will be restarted for logfile truncation`

Message Type: LOG

Severity: WARNING

Probable Cause: Indicates the size of the HTTP logfile exceeded the maximum limit.

Recommended Action: No action is required.

WEBD-1006

Message: `HTTP server and weblinker restarted due to logfile truncation`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates the size of the HTTP log file exceeded the maximum limit.

Recommended Action: No action is required.

WEBD-1007

Message: `HTTP server and weblinker process will be restarted due to change of IP Address`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates the IP address of the switch changed and the HTTP server is restarted.

Recommended Action: No action is required.

WEBD-1008

Message: `HTTP server and weblinker process cannot be started`

Message Type: LOG | FFDC

Severity: WARNING

Probable Cause: Indicates a rare error condition, where the built-in recovery process has failed to restore http services. The problem often results from invalid configuration of SSL certificates, but therecan be more than one reason for such a failure.

Recommended Action: Verify the certification file as there may be a mismatch involved.

WEBD-1009

Message: `<INFO %s>`

Message Type: LOG

Severity: INFO

Probable Cause: Indicates that the HTTP or HTTPS server configuration has changed.

Recommended Action: No action is required.