



EC Network Element Alarm Guide

Please Read

Important

Read this entire guide. If this guide provides installation or operation instructions, give particular attention to all safety statements included in this guide.

Notices

Trademark Acknowledgments

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks.

Third party trademarks mentioned are the property of their respective owners.

The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Publication Disclaimer

Cisco Systems, Inc. assumes no responsibility for errors or omissions that may appear in this publication. We reserve the right to change this publication at any time without notice. This document is not to be construed as conferring by implication, estoppel, or otherwise any license or right under any copyright or patent, whether or not the use of any information in this document employs an invention claimed in any existing or later issued patent.

Copyright

© 2014 Cisco and/or its affiliates. All rights reserved.

Information in this publication is subject to change without notice. No part of this publication may be reproduced or transmitted in any form, by photocopy, microfilm, xerography, or any other means, or incorporated into any information retrieval system, electronic or mechanical, for any purpose, without the express permission of Cisco Systems, Inc.

Contents

About This Guide

xiii

Chapter 1 QAM Modulator Alarms 1

QAM Modulator Alarm ID 0 (0 Hex).....	2
QAM Modulator Alarm ID 1 (1 Hex).....	3
QAM Modulator Alarm ID 2 (2 Hex).....	4
QAM Modulator Alarm ID 3 (3 Hex).....	5
QAM Modulator Alarm ID 4 (4 Hex).....	6
QAM Modulator Alarm ID 5 (5 Hex).....	7
QAM Modulator Alarm ID 7 (7 Hex).....	8
QAM Modulator Alarm ID 8 (8 Hex).....	9
QAM Modulator Alarm ID 9 (9 Hex).....	10
QAM Modulator Alarm ID 10 (A Hex).....	11
QAM Modulator Alarm ID 11 (B Hex).....	12
QAM Modulator Alarm ID 12 (C Hex).....	13
QAM Modulator Alarm ID 13 (D Hex).....	15
QAM Modulator Alarm ID 14 (E Hex).....	17
QAM Modulator Alarm ID 15 (F Hex).....	19
QAM Modulator Alarm ID 16 (10 Hex).....	20
QAM Modulator Alarm ID 17 (11 Hex).....	21
QAM Modulator Alarm ID 18 (12 Hex).....	22
QAM Modulator Alarm ID 19 (13 Hex).....	23
QAM Modulator Alarm ID 20 (14 Hex).....	24
QAM Modulator Alarm ID 21 (15 Hex).....	25
QAM Modulator Alarm ID 22 (16 Hex).....	27
QAM Modulator Alarm ID 23 (17 Hex).....	28
QAM Modulator Alarm ID 24 (18 Hex).....	29
QAM Modulator Alarm ID 25 (19 Hex).....	30
QAM Modulator Alarm ID 26 (1A Hex).....	31
QAM Modulator Alarm ID 27 (1B Hex).....	32

Chapter 2 MQAM Modulator Alarms 33

MQAM Modulator Alarm ID 1 (1 Hex).....	34
MQAM Modulator Alarm ID 2 (2 Hex).....	35
MQAM Modulator Alarm ID 3 (3 Hex).....	36
MQAM Modulator Alarm ID 4 (4 Hex).....	37
MQAM Modulator Alarm ID 5 (5 Hex).....	38
MQAM Modulator Alarm ID 6 (6 Hex).....	39
MQAM Modulator Alarm ID 7 (7 Hex).....	40
MQAM Modulator Alarm ID 8 (8 Hex).....	41

Contents

MQAM Modulator Alarm ID 9 (9 Hex).....	42
MQAM Modulator Alarm ID 10 (A Hex).....	43
MQAM Modulator Alarm ID 11 (B Hex).....	44
MQAM Modulator Alarm ID 13 (D Hex).....	45
MQAM Modulator Alarm ID 14 (E Hex).....	46
MQAM Modulator Alarm ID 15 (F Hex).....	47
MQAM Modulator Alarm ID 16 (10 Hex).....	48
MQAM Modulator Alarm ID 17 (11 Hex).....	49
MQAM Modulator Alarm ID 18 (12 Hex).....	50
MQAM Modulator Alarm ID 19 (13 Hex).....	51
MQAM Modulator Alarm ID 20 (14 Hex).....	52
MQAM Modulator Alarm ID 21 (15 Hex).....	53
MQAM Modulator Alarm ID 22 (16 Hex).....	54
MQAM Modulator Alarm ID 23 (17 Hex).....	55
MQAM Modulator Alarm ID 25 (19 Hex).....	56
MQAM Modulator Alarm ID 26 (1A Hex).....	57
MQAM Modulator Alarm ID 27 (1B Hex).....	58
MQAM Modulator Alarm ID 28 (1C Hex).....	59
MQAM Modulator Alarm ID 29 (1D Hex).....	60
MQAM Modulator Alarm ID 30 (1E Hex).....	61
MQAM Modulator Alarm ID 31 (1F Hex).....	62
MQAM Modulator Alarm ID 32 (20 Hex).....	63
MQAM Modulator Alarm ID 33 (21 Hex).....	64
MQAM Modulator Alarm ID 34 (22 Hex).....	65
MQAM Modulator Alarm ID 35 (23 Hex).....	66
MQAM Modulator Alarm ID 37 (25 Hex).....	67
MQAM Modulator Alarm ID 38 (26 Hex).....	68
MQAM Modulator Alarm ID 39 (27 Hex).....	69
MQAM Modulator Alarm ID 40 (28 Hex).....	70
MQAM Modulator Alarm ID 41 (29 Hex).....	71
MQAM Modulator Alarm ID 42 (2A Hex).....	72
MQAM Modulator Alarm ID 43 (2B Hex).....	73
MQAM Modulator Alarm ID 44 (2C Hex).....	74
MQAM Modulator Alarm ID 45 (2D Hex).....	75
MQAM Modulator Alarm ID 46 (2E Hex).....	76
MQAM Modulator Alarm ID 47 (2F Hex).....	77
MQAM Modulator Alarm ID 49 (31 Hex).....	78
MQAM Modulator Alarm ID 50 (32 Hex).....	79
MQAM Modulator Alarm ID 51 (33 Hex).....	81
MQAM Modulator Alarm ID 52 (34 Hex).....	82
MQAM Modulator Alarm ID 53 (35 Hex).....	83
MQAM Modulator Alarm ID 54 (36 Hex).....	85
MQAM Modulator Alarm ID 55 (37 Hex).....	87
MQAM Modulator Alarm ID 56 (38 Hex).....	89
MQAM Modulator Alarm ID 57 (39 Hex).....	90
MQAM Modulator Alarm ID 58 (3A Hex).....	92

MQAM Modulator Alarm ID 59 (3B Hex)	94
MQAM Modulator Alarm ID 60 (3C Hex)	96
MQAM Modulator Alarm ID 61 (3D Hex)	98
MQAM Modulator Alarm ID 62 (3E Hex)	100
MQAM Modulator Alarm ID 63 (3F Hex)	102
MQAM Modulator Alarm ID 64 (40 Hex)	104
MQAM Modulator Alarm ID 65 (41 Hex)	105
MQAM Modulator Alarm ID 66 (42 Hex)	106
MQAM Modulator Alarm ID 67 (43 Hex)	107
MQAM Modulator Alarm ID 68 (44 Hex)	108
MQAM Modulator Alarm ID 69 (45 Hex)	109
MQAM Modulator Alarm ID 70 (46 Hex)	110
MQAM Modulator Alarm ID 71 (47 Hex)	111
MQAM Modulator Alarm ID 72 (48 Hex)	112
MQAM Modulator Alarm ID 73 (49 Hex)	113
MQAM Modulator Alarm ID 74 (4A Hex)	114
MQAM Modulator Alarm ID 75 (4B Hex)	115
MQAM Modulator Alarm ID 76 (4C Hex)	116
MQAM Modulator Alarm ID 77 (4D Hex)	117
MQAM Modulator Alarm ID 78 (4E Hex)	118
MQAM Modulator Alarm ID 79 (4F Hex)	119
MQAM Modulator Alarm ID 128 (80 Hex) through Alarm ID 1151 (47F Hex)	120
MQAM Modulator Alarm ID 1152 (480 Hex) through Alarm ID 2175 (87F Hex)	123
MQAM Modulator Alarm ID 2176 (880 Hex) through Alarm ID 3199 (C7F Hex)	125

Chapter 3 GQAM Modulator Alarms 127

GQAM Modulator Alarm ID 1 (1 Hex)	128
GQAM Modulator Alarm ID 2 (2 Hex)	129
GQAM Modulator Alarm ID 3 (3 Hex)	130
GQAM Modulator Alarm ID 4 (4 Hex)	131
GQAM Modulator Alarm ID 5 (5 Hex)	132
GQAM Modulator Alarm ID 7 (7 Hex)	133
GQAM Modulator Alarm ID 8 (8 Hex)	134
GQAM Modulator Alarm ID 9 (9 Hex)	135
GQAM Modulator Alarm ID 10 (A Hex)	136
GQAM Modulator Alarm ID 11 (B Hex)	137
GQAM Modulator Alarm ID 12 (C Hex)	138
GQAM Modulator Alarm ID 13 (D Hex)	139
GQAM Modulator Alarm ID 14 (E Hex)	140
GQAM Modulator Alarm ID 15 (F Hex)	141
GQAM Modulator Alarm ID 17 (11 Hex)	142
GQAM Modulator Alarm ID 18 (12 Hex)	143
GQAM Modulator Alarm ID 19 (13 Hex)	144
GQAM Modulator Alarm ID 20 (14 Hex)	145
GQAM Modulator Alarm ID 21 (15 Hex)	146
GQAM Modulator Alarm ID 22 (16 Hex)	147

Contents

GQAM Modulator Alarm ID 23 (17 Hex).....	148
GQAM Modulator Alarm ID 24 (18 Hex).....	149
GQAM Modulator Alarm ID 25 (19 Hex).....	150
GQAM Modulator Alarm ID 27 (1B Hex).....	151
GQAM Modulator Alarm ID 28 (1C Hex).....	152
GQAM Modulator Alarm ID 29 (1D Hex).....	153
GQAM Modulator Alarm ID 30 (1E Hex).....	154
GQAM Modulator Alarm ID 31 (1F Hex).....	155
GQAM Modulator Alarm ID 32 (20 Hex).....	156
GQAM Modulator Alarm ID 33 (21 Hex).....	157
GQAM Modulator Alarm ID 34 (22 Hex).....	158
GQAM Modulator Alarm ID 35 (23 Hex).....	159
GQAM Modulator Alarm ID 37 (25 Hex).....	160
GQAM Modulator Alarm ID 38 (26 Hex).....	161
GQAM Modulator Alarm ID 39 (27 Hex).....	162
GQAM Modulator Alarm ID 40 (28 Hex).....	163
GQAM Modulator Alarm ID 41 (29 Hex).....	164
GQAM Modulator Alarm ID 42 (2A Hex).....	165
GQAM Modulator Alarm ID 43 (2B Hex).....	167
GQAM Modulator Alarm ID 44 (2C Hex).....	168
GQAM Modulator Alarm ID 45 (2D Hex).....	170
GQAM Modulator Alarm ID 46 (2E Hex).....	171
GQAM Modulator Alarm ID 47 (2F Hex).....	173
GQAM Modulator Alarm ID 48 (30 Hex).....	174
GQAM Modulator Alarm ID 49 (31 Hex).....	176
GQAM Modulator Alarm ID 50 (32 Hex).....	177
GQAM Modulator Alarm ID 51 (33 Hex).....	179
GQAM Modulator Alarm ID 52 (34 Hex).....	180
GQAM Modulator Alarm ID 53 (35 Hex).....	181
GQAM Modulator Alarm ID 54 (36 Hex).....	183
GQAM Modulator Alarm ID 55 (37 Hex).....	185
GQAM Modulator Alarm ID 56 (38 Hex).....	187
GQAM Modulator Alarm ID 57 (39 Hex).....	188
GQAM Modulator Alarm ID 58 (3A Hex).....	190
GQAM Modulator Alarm ID 59 (3B Hex).....	192
GQAM Modulator Alarm ID 60 (3C Hex).....	194
GQAM Modulator Alarm ID 61 (3D Hex).....	195
GQAM Modulator Alarm ID 62 (3E Hex).....	197
GQAM Modulator Alarm ID 63 (3F Hex).....	199
GQAM Modulator Alarm ID 64 (40 Hex).....	201
GQAM Modulator Alarm ID 65 (41 Hex).....	202
GQAM Modulator Alarm ID 66 (42 Hex).....	204
GQAM Modulator Alarm ID 67 (43 Hex).....	206
GQAM Modulator Alarm ID 68 (44 Hex).....	208
GQAM Modulator Alarm ID 69 (45 Hex).....	209
GQAM Modulator Alarm ID 70 (46 Hex).....	211

GQAM Modulator Alarm ID 71 (47 Hex).....	213
GQAM Modulator Alarm ID 72 (48 Hex).....	215
GQAM Modulator Alarm ID 73 (49 Hex).....	217
GQAM Modulator Alarm ID 74 (4A Hex)	219
GQAM Modulator Alarm ID 75 (4B Hex)	221
GQAM Modulator Alarm ID 76 (4C Hex).....	223
GQAM Modulator Alarm ID 77 (4D Hex).....	225
GQAM Modulator Alarm ID 78 (4E Hex)	227
GQAM Modulator Alarm ID 79 (4F Hex)	229
GQAM Modulator Alarm ID 80 (50 Hex).....	231
GQAM Modulator Alarm ID 81 (51 Hex).....	233
GQAM Modulator Alarm ID 82 (52 Hex).....	235
GQAM Modulator Alarm ID 83 (53 Hex).....	237
GQAM Modulator Alarm ID 84 (54 Hex).....	239
GQAM Modulator Alarm ID 85 (55 Hex).....	241
GQAM Modulator Alarm ID 86 (56 Hex).....	243
GQAM Modulator Alarm ID 87 (57 Hex).....	245
GQAM Modulator Alarm ID 88 (58 Hex).....	247
GQAM Modulator Alarm ID 89 (59 Hex).....	248
GQAM Modulator Alarm ID 90 (5A Hex)	249
GQAM Modulator Alarm ID 91 (5B Hex)	250
GQAM Modulator Alarm ID 92 (5C Hex).....	251
GQAM Modulator Alarm ID 93 (5D Hex).....	252
GQAM Modulator Alarm ID 94 (5E Hex)	253
GQAM Modulator Alarm ID 95 (5F Hex)	254
GQAM Modulator Alarm ID 96 (60 Hex).....	255
GQAM Modulator Alarm ID 97 (61 Hex).....	256
GQAM Modulator Alarm ID 98 (62 Hex).....	257
GQAM Modulator Alarm ID 99 (63 Hex).....	258
GQAM Modulator Alarm ID 100 (64 Hex).....	259
GQAM Modulator Alarm ID 101 (65 Hex).....	260
GQAM Modulator Alarm ID 102 (66 Hex).....	261
GQAM Modulator Alarm ID 103 (67 Hex).....	262
GQAM Modulator Alarm ID 104 (68 Hex).....	263
GQAM Modulator Alarm ID 105 (69 Hex).....	264
GQAM Modulator Alarm ID 106 (6A Hex)	265
GQAM Modulator Alarm ID 107 (6B Hex)	266
GQAM Modulator Alarm ID 108 (6C Hex).....	267
GQAM Modulator Alarm ID 109 (6D Hex).....	268
GQAM Modulator Alarm ID 110 (6E Hex)	269
GQAM Modulator Alarm ID 111 (6F Hex)	270
GQAM Modulator Alarm ID 112 (70 Hex).....	271
GQAM Modulator Alarm ID 113 (71 Hex).....	272
GQAM Modulator Alarm ID 256 (100 Hex) through Alarm ID 1247 (4DF Hex)	273
GQAM Modulator Alarm ID 1280 (500 Hex) through Alarm ID 2271 (8DF Hex)	276
GQAM Modulator Alarm ID 2304 (900 Hex) through Alarm ID 3295 (CDF Hex).....	278
GQAM Modulator Alarm ID 3328 (D00 Hex) through Alarm ID 4351 (10FF Hex) ...	280

Chapter 4 Netcrypt Alarms	281
Netcrypt Alarm ID 0 (0 Hex).....	282
Netcrypt Alarm ID 1 (1 Hex).....	283
Netcrypt Alarm ID 2 (2 Hex).....	285
Netcrypt Alarm ID 3 (3 Hex).....	286
Netcrypt Alarm ID 4 (4 Hex).....	288
Netcrypt Alarm ID 5 (5 Hex).....	289
Netcrypt Alarm ID 6 (6 Hex).....	291
Netcrypt Alarm ID 7 (7 Hex).....	292
Netcrypt Alarm ID 8 (8 Hex).....	294
Netcrypt Alarm ID 17 (11 Hex).....	295
Netcrypt Alarm ID 18 (12 Hex).....	296
Netcrypt Alarm ID 19 (13 Hex).....	298
Netcrypt Alarm ID 20 (14 Hex).....	299
Netcrypt Alarm ID 21 (15 Hex).....	301
Netcrypt Alarm ID 22 (16 Hex).....	302
Netcrypt Alarm ID 23 (17 Hex).....	304
Netcrypt Alarm ID 24 (18 Hex).....	305
Netcrypt Alarm ID 25 (19 Hex).....	307
Netcrypt Alarm ID 26 (1A Hex).....	308
Netcrypt Alarm ID 27 (1B Hex).....	310
Netcrypt Alarm ID 28 (1C Hex).....	311
Netcrypt Alarm ID 29 (1D Hex).....	313
Netcrypt Alarm ID 30 (1D Hex).....	314
Netcrypt Alarm ID 31 (1F Hex).....	316
Netcrypt Alarm ID 32 (20 Hex).....	317
Netcrypt Alarm ID 49 (31 Hex).....	319
Netcrypt Alarm ID 50 (32 Hex).....	320
Netcrypt Alarm ID 51 (33 Hex).....	321
Netcrypt Alarm ID 52 (34 Hex).....	322
Netcrypt Alarm ID 57 (39 Hex).....	323
Netcrypt Alarm ID 58 (3A Hex).....	324
Netcrypt Alarm ID 59 (3B Hex).....	325
Netcrypt Alarm ID 60 (3C Hex).....	326
Netcrypt Alarm ID 61 (3D Hex).....	327
Netcrypt Alarm ID 62 (3E Hex).....	328
Netcrypt Alarm ID 63 (3F Hex).....	329
Netcrypt Alarm ID 64 (40 Hex).....	330
Netcrypt Alarm ID 73 (49 Hex).....	331
Netcrypt Alarm ID 74 (4A Hex).....	332
Netcrypt Alarm ID 75 (4B Hex).....	333
Netcrypt Alarm ID 76 (4C Hex).....	334
Netcrypt Alarm ID 78 (4E Hex).....	335
Netcrypt Alarm ID 79 (4F Hex).....	336

Netcrypt Alarm ID 80 (50 Hex).....	337
Netcrypt Alarm ID 81 (51 Hex).....	338
Netcrypt Alarm ID 82 (52 Hex).....	339
Netcrypt Alarm ID 83 (53 Hex).....	340
Netcrypt Alarm ID 84 (54 Hex).....	341
Netcrypt Alarm ID 85 (55 Hex).....	342
Netcrypt Alarm ID 86 (56 Hex).....	343
Netcrypt Alarm ID 87 (57 Hex).....	344
Netcrypt Alarm ID 88 (58 Hex).....	345
Netcrypt Alarm ID 89 (59 Hex).....	346
Netcrypt Alarm ID 99 (63 Hex).....	347
Netcrypt Alarm ID 100 (64 Hex).....	349
Netcrypt Alarm ID 101 (65 Hex).....	351
Netcrypt Alarm ID 102 (66 Hex).....	353
Netcrypt Alarm ID 108 (6C Hex).....	355
Netcrypt Alarm ID 109 (6D Hex).....	356
Netcrypt Alarm ID 110 (6E Hex).....	357
Netcrypt Alarm ID 111 (6F Hex).....	358
Netcrypt Alarm ID 116 (74 Hex).....	359
Netcrypt Alarm ID 117 (75 Hex).....	360
Netcrypt Alarm ID 118 (76 Hex).....	361
Netcrypt Alarm ID 119 (77 Hex).....	362
Netcrypt Alarm ID 120 (78 Hex).....	363
Netcrypt Alarm ID 121 (79 Hex).....	364
Netcrypt Alarm ID 122 (7A Hex).....	365
Netcrypt Alarm ID 123 (7B Hex).....	366
Netcrypt Alarm ID 124 (7C Hex).....	367
Netcrypt Alarm ID 125 (7D Hex).....	368
Netcrypt Alarm ID 126 (7E Hex).....	369
Netcrypt Alarm ID 127 (7F Hex).....	370
Netcrypt Alarm ID 128 (80 Hex).....	371
Netcrypt Alarm ID 129 (81 Hex).....	372
Netcrypt Alarm ID 256 (100 Hex) through Alarm ID 4255 (109F Hex).....	373
Netcrypt Alarm ID 4256 (10A0) Hex) through Alarm ID 8255 (203F) Hex.....	376
Netcrypt Alarm ID 8256 (2040 Hex) through Alarm ID 12255 (2FDF Hex).....	378

Chapter 5 QPSK Modulator Alarms 381

QPSK Modulator Alarm ID 0 (0 Hex).....	382
QPSK Modulator Alarm ID 1 (1 Hex).....	383
QPSK Modulator Alarm ID 2 (2 Hex).....	384
QPSK Modulator Alarm ID 3 (3 Hex).....	385
QPSK Modulator Alarm ID 4 (4 Hex).....	386
QPSK Modulator Alarm ID 5 (5 Hex).....	388
QPSK Modulator Alarm ID 7 (7 Hex).....	390
QPSK Modulator Alarm 256 (100 Hex).....	391
QPSK Modulator Alarm ID 257 (101 Hex).....	393

Contents

QPSK Modulator Alarm ID 258 (102 Hex)	396
QPSK Modulator Alarm ID 259 (103 Hex)	399
QPSK Modulator Alarm ID 260 (104 Hex)	402
QPSK Modulator Alarm ID 261 (105 Hex)	403
QPSK Modulator Alarm ID 263 (107 Hex)	404
QPSK Modulator Alarm ID 264 (108 Hex)	405
QPSK Modulator Alarm ID 265 (109 Hex)	409
QPSK Modulator Alarm ID 512 (200 Hex)	412
QPSK Modulator Alarm ID 515 (203 Hex)	413
QPSK Modulator Alarm ID 519 (207 Hex)	415
QPSK Modulator Alarm ID 522 (20A Hex)	416
QPSK Modulator Alarm ID 523 (20B Hex)	417
QPSK Modulator Alarm ID 524 (20C Hex)	419
QPSK Modulator Alarm ID 1024 (400 Hex)	420
QPSK Modulator Alarm ID 1280 (500 Hex)	421
QPSK Modulator Alarm ID 1284 (504 Hex)	422
QPSK Modulator Alarm ID 1285 (505 Hex)	423
QPSK Modulator Alarm ID 1286 (506 Hex)	424
QPSK Modulator Alarm ID 1287 (507 Hex)	426
QPSK Modulator Alarm ID 1288 (508 Hex)	427
QPSK Modulator Alarm ID 1291 (50B Hex)	428

Chapter 6 QPSK Demodulator Alarms **429**

QPSK Demodulator Alarm ID 0 (0 Hex)	430
QPSK Demodulator Alarm ID 1 (1 Hex)	431
QPSK Demodulator Alarm ID 2 (2 Hex)	432
QPSK Demodulator Alarm ID 3 (3 Hex)	433
QPSK Demodulator Alarm ID 4 (4 Hex)	434
QPSK Demodulator Alarm ID 5 (5 Hex)	435
QPSK Demodulator Alarm ID 6 (6 Hex)	436
QPSK Demodulator Alarm ID 7 (7 Hex)	437
QPSK Demodulator Alarm ID 8 (8 Hex)	438
QPSK Demodulator Alarm ID 9 (9 Hex)	439
QPSK Demodulator Alarm 10 (A Hex)	440
QPSK Demodulator Alarm ID 11 (B Hex)	442
QPSK Demodulator Alarm ID 12 (C Hex)	443
QPSK Demodulator Alarm ID 13 (D Hex)	444
QPSK Demodulator Alarm ID 14 (E Hex)	445
QPSK Demodulator Alarm ID 15 (F Hex)	446
QPSK Demodulator Alarm ID 16 (10 Hex)	447
QPSK Demodulator Alarm ID 17 (11 Hex)	448
QPSK Demodulator Alarm ID 18 (12 Hex)	449
QPSK Demodulator Alarm ID 19 (13 Hex)	450
QPSK Demodulator Alarm ID 20 (14 Hex)	451
QPSK Demodulator Alarm ID 23 (17 Hex)	452

Chapter 7 Customer Information

453

About This Guide

Introduction

This guide lists and describes the network element alarms that are associated with the Explorer Controller (EC).

Document Version

This is the first formal release of this document.

1

QAM Modulator Alarms

Introduction

This chapter provides detailed information for troubleshooting the alarms that are generated by the QAM modulator. The alarms are arranged in the ascending numeric order of the Alarm IDs. For your convenience, the Alarm IDs are listed in both decimal and hexadecimal format. You can look up the possible causes and then follow the check and correct procedures for each alarm to help you troubleshoot and clear each alarm.

 QAM modulators do not support Session alarms.

QAM Modulator Alarm ID 0 (0 Hex)

The **SMC Communication Failure** alarm occurs when the system is unable to communicate with the QAM modulator board while polling for SMC, or for setting provisioning information. There is a potential for loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the QAM modulator that is sending this alarm.

Front Panel Message

SMC communication failed

Possible Cause(s)

- A cable is loose, disconnected, or defective.
- Hardware failure occurred.

Check and Correct

Loose, disconnected, or defective cables

Check for loose connections or defective cables, tighten any loose cable connections, connect any disconnected cables, and replace any defective cables.

Hardware failure

- 1 Replace the QAM modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the QAM modulator.
- 2 If the alarm condition continues to occur, contact Cisco Services.

QAM Modulator Alarm ID 1 (1 Hex)

The **Excessive Temperature** alarm occurs when the internal temperature of the QAM modulator exceeds 70°C (158°F). A QAM modulator that is overheating could have minimal to severe impact on services. If the QAM modulator fails due to overheating, there would be no services available from that QAM modulator.

Front Panel Message

Exceeded Max Temp

Possible Cause(s)

- The vents on the QAM modulator are blocked.
- The room temperature is too high.
- A fan failure occurred.
- A hardware failure occurred.

Check and Correct

Vents are blocked

Check and clear any obstructions from the vents.

Room temperature too high

Check and repair or replace the heating/cooling equipment in the room.

Fan failure

Check and repair or replace the fan.

Hardware failure

- 1 Replace the QAM modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the QAM modulator.
- 2 If the alarm condition continues to occur, contact Cisco Services.

QAM Modulator Alarm ID 2 (2 Hex)

The **Power Supply Failure** alarm occurs when the power supply is out of specifications or is not operating correctly. No services are available from this QAM (*javascript:kadovTextPopup(this)*) modulator.

Front Panel Message

Power supply failed

Possible Cause(s)

The internal power supply in the QAM modulator has failed or is failing.

Check and Correct

- 1 Check power source, power wires, and the on/off switch on the back panel of the QAM modulator.
- 2 Replace the QAM modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the QAM modulator.
- 3 If the alarm continues to occur, contact Cisco Services for further assistance.

QAM Modulator Alarm ID 3 (3 Hex)

The **Lock Detect Failure** alarm occurs when the synthesizer lock-detect circuitry fails. There is potential loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the QAM modulator that is sending this alarm.

Front Panel Message

Lock detect logic failed

Possible Cause(s)

Hardware failure occurred.

Check and Correct

- 1 Power down and then power up the QAM modulator using the on/off rocker-type switch on the back panel, or reset the QAM modulator from the DNCS.
- 2 Replace the QAM modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the QAM modulator.
- 3 If the alarm continues to occur, contact Cisco Services for further assistance.

QAM Modulator Alarm ID 4 (4 Hex)

The **PLL Unlocked** alarm occurs when the synthesizer PLL cannot lock. There is potential loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the QAM modulator that is sending this alarm.

Front Panel Message

PLL unlocked

Possible Cause(s)

Hardware failure occurred.

Check and Correct

- 1 Power down and then power up the QAM modulator using the on/off rocker-type switch on the back panel, or reset the QAM modulator from the DNCS.
- 2 Replace the QAM modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the QAM modulator.
- 3 If the alarm continues to occur, contact Cisco Services for further assistance.

QAM Modulator Alarm ID 5 (5 Hex)

The **RAM Self-Test Failure** alarm occurs when the NVRAM self-test in the QAM modulator fails. No services are available from this QAM modulator.

Front Panel Message

NVM failed

Possible Cause(s)

Hardware failure occurred.

Check and Correct

- 1 Replace the QAM modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the QAM modulator.
- 2 If the alarm continues to occur, contact Cisco Services for further assistance.

QAM Modulator Alarm ID 7 (7 Hex)

The **ASIC Initialization Failure** alarm occurs when the ASIC chip fails to initialize. No services are available from this QAM modulator.

Front Panel Message

Mod ASIC init failed

Possible Cause(s)

Hardware failure occurred

Check and Correct

- 1 Power down and then power up the QAM modulator using the on/off rocker-type switch on the back panel, or reset the QAM modulator from the DNCS.
- 2 Replace the QAM modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the QAM modulator.
- 3 If the alarm continues to occur, contact Cisco Services for further assistance.

QAM Modulator Alarm ID 8 (8 Hex)

The **Power Supply Low** alarm occurs when the 24 V DC power supply is out of specification but has not failed. There is potential loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the QAM modulator that is sending this alarm.

Front Panel Message

24 volt supply low

Possible Causes

- A power connection is loose, disconnected, or defective.
- There is low voltage at the power outlet.
- A hardware failure occurred.

Check and Correct

Power connection loose, disconnected, or defective

- 1 Check for loose connections or defective cables, tighten any loose cable connections, connect any disconnected cables, and replace any defective cables.
- 2 Check for defective cables and replace any defective cables.

Low voltage

Check the voltage levels at the power outlet to verify that the levels are correct.

Hardware failure

- 1 Replace the QAM modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the QAM modulator.
- 2 If the alarm continues to occur, contact Cisco Services for further assistance.

QAM Modulator Alarm ID 9 (9 Hex)

The **Calibration Error** alarm occurs when the QAM modulator level is not calibrated to its frequency. The QAM modulator continues to operate, but the RF level may vary beyond specified limits (as much as ± 3 dB) when the output frequency changes. There is potential loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the QAM modulator that is sending this alarm.

Front Panel Message

Level not calibrated

Possible Cause(s)

The QAM modulator is not calibrated to the correct frequency.

Check and Correct

- 1 Power down and then power up the QAM modulator using the on/off rocker-type switch on the back panel, or reset the QAM modulator from the DNCS.
- 2 Replace the QAM modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the QAM modulator.
- 3 If the alarm continues to occur, contact Cisco Services for further assistance.

QAM Modulator Alarm ID 10 (A Hex)

The **SMC Communication Error** alarm occurs when the QAM modulator detects a problem with SMC during initialization or operation. There is a potential for loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the QAM modulator that is sending this alarm.

Front Panel Message

SMC communication failed

Possible Cause(s)

- A cable is loose, disconnected, or defective.
- Hardware failure or software bugs occurred.

Check and Correct

Loose, disconnected, or defective cables

Check for loose connections or defective cables, tighten any loose cable connections, connect any disconnected cables, and replace any defective cables.

Hardware failure or software bugs

- 1 Power down and then power up the QAM modulator using the on/off rocker-type switch on the back panel, or reset the QAM modulator from the DNCS.
- 2 Replace the QAM modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the QAM modulator.
- 3 If the alarm continues to occur, contact Cisco Services for further assistance.

QAM Modulator Alarm ID 11 (B Hex)

The **Front Panel Changed** status event occurs when a user or a system operator changes provisioning parameters on the QAM modulator using the front panel keys. There is a potential for loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the QAM modulator that is sending this alarm.

Front Panel Message

Front panel changed

Possible Causes(s)

A user or a system operator entered new provisioning parameters on the QAM modulator using the front panel keys.

Check and Correct

- 1 Verify what settings were changed.
- 2 Are all services functioning correctly?
 - If **yes**, no further action is required.
 - If **no**, go to step 3.
- 3 Restore the settings to the previous configuration.
- 4 Power down and then power up the QAM modulator using the on/off rocker-type switch on the back panel, or reset the QAM modulator from the DNCS to restore the previous configuration.
- 5 If resetting the QAM modulator does not solve the problem, contact Cisco Services for further assistance.

QAM Modulator Alarm ID 12 (C Hex)

The **Loss of Signal Error** occurs when the carrier detect bit for the installed DHEI, SWIF, or DVB ASI interface is not active. None of the bits indicating one of the three input ports (DHEI, SWIF, or DVB ASI) is active. No services are available from this QAM modulator when this alarm occurs.

Important! This alarm also appears and immediately clears when the QAM modulator is powered off and then powered on from the back panel.

Note: There is no impact to the system when this alarm occurs and then immediately clears after the QAM modulator is powered off and then powered on from the back panel.

Front Panel Message

Loss of input signal

Possible Causes(s)

- The QAM modulator was powered off and then powered on from the back panel.
- A cable is loose, disconnected, or defective.
- The incorrect input is selected on the DNCS and on the front panel LCD of the QAM modulator.
- An upstream device providing input to the QAM modulator failed or is offline.
- The QAM modulator is defective.

Check and Correct

QAM modulator powered off and powered on from back panel

No action is required since the alarm automatically clears in this situation.

Loose, disconnected, or defective cables

Check for loose connections or defective cables, tighten any loose cable connections, connect any disconnected cables, and replace any defective cables.

Incorrect input selected

Verify that the correct input source is selected on the DNCS and on the front panel LCD of the QAM modulator.

Chapter 1 QAM Modulator Alarms

Upstream device failed or is off line

- 1 Verify that the source devices that are providing content to the QAM modulator are functioning correctly.
- 2 Run the Doctor Report on the DNCS, and examine the report for any network connectivity issues or indications of loss of service.
- 3 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 4 If the alarm continues to occur, contact Cisco Services for further assistance

QAM modulator is defective

- 1 Replace the QAM modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the QAM modulator.
- 2 If the alarm continues to occur, contact Cisco Services for further assistance.

QAM Modulator Alarm ID 13 (D Hex)

The **MPEG Packets Error** alarm occurs when the QAM modulator detects errored MPEG packets. There is potential loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the QAM modulator that is sending this alarm.

Notes:

- This alarm appears when the DVB ASI cable is loose, disconnected, or defective.
- This alarm appears and immediately clears when either the SWIF cable or the ECL cable is disconnected and then re-connected.

Front Panel Message

Errored MPEG Packets

Possible Cause(s)

- The DVB ASI cable is loose, disconnected, or defective.
- The SWIF cable or the ECL cable was disconnected and then re-connected.
- There are data errors on the satellite link.
- The rate of change of the IEC exceeds the allowed threshold.
- There is defective upstream equipment or failure on the input data link of the QAM modulator.
- There is defective local MPEG coding.
- The QAM modulator is defective.

Check and Correct

DVB ASI cable is loose, disconnected, or defective

Check for loose DVB ASI cable connections or defective cables, tighten any loose connections, and replace any defective cables.

SWIF cable or ECL cable was disconnected and then re-connected

No action is required since this alarm automatically clears in this situation

Satellite link data errors

Contact your signal provider to verify if there are any problems with their satellite transmissions.

IEC errors

Clean up the MPEG signal input to the QAM modulator by checking the IRT, RTE, and MPEG encoder.

Chapter 1 QAM Modulator Alarms

Defective upstream equipment

- 1 Check the upstream devices that are sending MPEG packets to the QAM modulator.
- 2 Run the Doctor Report on the DNCS, and examine the report for any network connectivity issues or indications of loss of service.
- 3 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 4 If the alarm continues to occur, contact Cisco Services for further assistance

Defective local MPEG coding

Check the local source devices that are providing MPEG content to the QAM modulator.

QAM modulator is defective

- 1 Replace the QAM modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the QAM modulator.
- 2 If the alarm continues to occur, contact Cisco Services for further assistance.

QAM Modulator Alarm ID 14 (E Hex)

The **FIFO Overflow Error** alarm occurs when the QAM modulator detects a FIFO overflow error, and packet data is lost. There is a potential for loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the QAM modulator that is sending this alarm.

Front Panel Message

FIFO Overflow

Possible Cause(s)

- The data rate as defined from the DNCS for the QAM modulator sessions is too low, which also means that the data rate of the input to the QAM modulator is too high.
- There are too many sessions defined for the QAM modulator from the DNCS.
- The modulation mode is incorrect.
- Upstream devices are sending too many MPEG packets to the QAM modulator.
- A hardware failure occurred.

Check and Correct

Data rate defined from DNCS is too low

- 1 Follow these steps to reduce the data rate of the input to the QAM modulator:
- 2 Reduce the amount of incoming data.
- 3 Reduce the amount of data added to the stream.
- 4 Increase the QAM modulation mode.
- 5 Verify and correct session rate targets and threshold values.

Too many sessions defined

Reduce the total number of MPEG programs by deleting sessions.

Modulation mode incorrect

Verify and correct the modulation mode.

Upstream devices sending too many MPEG packets

Check the upstream devices that are sending MPEG packets to the input ports in the QAM modulator.

Chapter 1 QAM Modulator Alarms

Hardware failure occurred

- 1 Run the Doctor Report on the DNCS, and examine the report for any network connectivity issues or indications of loss of service.
- 2 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 3 Replace the QAM modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the QAM modulator.
- 4 If the alarm continues to occur, contact Cisco Services for further assistance.

QAM Modulator Alarm ID 15 (F Hex)

The **Interface Error** alarm occurs when the number of errored packets arriving at the QAM modulator MPEG input ports exceeds the allowed pre-defined threshold. There is a potential for loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality and other degradations to service relative to the QAM modulator that is sending this alarm.

Notes:

This alarm appears and immediately clears when the QAM modulator is powered off and powered on from the back panel. There is no impact to the system when this alarm occurs and then immediately clears after the QAM modulator powered of and powered on from the back panel.

This alarm appears when the DVB ASI cable is loose, disconnected, or defective.

This alarm appears and immediately clears when either the SWIF cable or the ECL cable is disconnected and then re-connected.

Front Panel Message

Interface error

Possible Cause(s)

- The QAM modulator was powered off and powered on from the back panel.
- The DVB ASI cable is loose, disconnected, or defective.
- The SWIF cable or ECL cable was disconnected and then re-connected.
- Packet errors, such as sync byte errors, packet size errors, and PMT CRC errors have exceeded the set threshold for the IEC.

Check and Correct

QAM Modulator powered off and powered on from the back panel

No action is required since this alarm automatically clears in this situation.

DVB ASI cable loose, disconnected, or defective

Check for loose DVB ASI connections or defective cables, tighten any loose cable connections, connect any disconnected cables, and replace any defective cables.

SWIF cable or ECL cable was disconnected and then re-connected

No action is required since this alarm automatically clears in this situation.

Packet errors exceed IEC threshold

- 1 Clean up the MPEG input signal to the QAM modulator.
- 2 If the alarm continues to occur, contact Cisco Services for further assistance.

QAM Modulator Alarm ID 16 (10 Hex)

The **Excess Packets Dumped** alarm occurs when too much data is entering the QAM modulator and excess packets are discarded. There is a potential for loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality and other degradations to service relative to the QAM modulator that is sending this alarm.

Front Panel Message

Packets were dumped

Possible Cause(s)

- The data rate as defined from the DNCS for the QAM modulator sessions is too low, which also means that the data rate of the input to the QAM modulator is too high.
- There are too many sessions defined for the QAM modulator from the DNCS.
- The modulation mode is incorrect.
- A hardware failure occurred.

Check and Correct

Data rate as defined from the DNCS is too low

- 1 Follow these steps to reduce the data rate of the input to the QAM modulator:
- 2 Reduce the amount of incoming data.
- 3 Reduce the amount of data added to the stream.
- 4 Increase the QAM modulation mode.
- 5 Verify and correct session rate targets and threshold values.

Too many sessions defined

Reduce the total number of MPEG programs by deleting sessions.

Modulation mode is incorrect

Verify and correct the modulation mode.

Hardware failure occurred

- 1 Run the Doctor Report on the DNCS, and examine the report for any network connectivity issues or indications of loss of service.
- 2 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 3 Replace the QAM modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the QAM modulator.
- 4 If the alarm continues to occur, contact Cisco Services for further assistance.

QAM Modulator Alarm ID 17 (11 Hex)

The **Reset Detected** alarm occurs when the QAM modulator is powered on or reset. There is a potential for loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality and other degradations to service relative to the QAM modulator that is sending this alarm.

Important! The following alarms may also appear and quickly clear when the QAM modulator is powered on or reset.

QAM Modulator Alarm ID 12 (C Hex) (on page 13)

QAM Modulator Alarm ID 13 (D Hex) (on page 15)

QAM Modulator Alarm ID 15 (F Hex) (on page 19)

QAM Modulator Alarm ID 19 (13 Hex) (on page 23)

Front Panel Message

Power-up/Reset

Possible Cause(s)

- Power was lost.
- The QAM modulator is initializing after being powered on or reset

Check and Correct

Power lost or device reset

- 1 Verify that the reset was intentional.
- 2 Send session and alarm provisioning data to the QAM modulator again.
- 3 Verify that all sessions recover successfully.
- 4 Check the channels assigned to this QAM modulator and verify that all services are still available.
- 5 If the QAM modulator sending the alarm is the BFS QAM, verify that the third day of the IPG is available, and then purchase a PPV event.
- 6 If the alarm continues to occur, contact Cisco Services for further assistance.

QAM Modulator Alarm ID 18 (12 Hex)

The **Hardware Error** alarm occurs when the QAM modulator detects a hardware error when accessing data through the SPI port or the CPU. Performance data retrieved through the craft port may be invalid. There is a potential for loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the QAM modulator that is sending this alarm.

Front Panel Message

Hardware error

Possible Cause(s)

The SPI to QAM modulator interface is in error, possibly caused by timing problems related to total SPI, Ethernet, and serial traffic.

Check and Correct

- 1 Power down and then power up QAM modulator using the on/off rocker-type switch on the back panel, and then reset the QAM modulator from the DNCS.
- 2 Replace the QAM modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the QAM modulator.
- 3 If the alarm continues to occur, contact Cisco Services for further assistance.

QAM Modulator Alarm ID 19 (13 Hex)

The **Runtime Error** alarm occurs when there low-level software errors in the QAM modulator. There is a potential for loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the QAM modulator that is sending this alarm.

Important! This alarm also appears and immediately clears when the QAM modulator is powered off and then powered on from the back panel.

Note: There is no impact to the system when this alarm occurs and then immediately clears after the QAM modulator is powered off and then powered on from the back panel.

Front Panel Message

Runtime error

Possible Cause(s)

- The QAM modulator was powered off and then powered on from the back panel.
- Low level software errors occurred.

Check and Correct

QAM modulator powered off and powered on from the back panel

No action is required since the alarm automatically clears in this situation.

Low level software errors occurred

- 1 Reset the QAM modulator from the DNCS.
- 2 Replace the QAM modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the QAM modulator.
- 3 If the alarm continues to occur, contact Cisco Services for further assistance.

QAM Modulator Alarm ID 20 (14 Hex)

The **Craft Port Activity** alarm occurs when an operator is using the craft port on the QAM modulator.

Front Panel Message

Craft event change

Possible Cause(s)

A device connected to the craft port sent a command to the QAM modulator.

Check and Correct

Disconnect the device from the craft port.

QAM Modulator Alarm ID 21 (15 Hex)

The **MPEG Continuity Error** alarm can occur when individual MPEG packets become corrupted due to random noise in the network. Each MPEG packet has a section for continuity bits that should contain a sequential value. These MPEG continuity bits are used by the MPEG packet recipient to verify that the packets in an MPEG stream are received in the correct sequential order and to verify that no packet loss has occurred.

This alarm also occurs when the QAM modulator receives packets in the MPEG stream that do not contain MPEG continuity bits.

There is a potential for loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the QAM modulator that is sending this alarm.

Notes:

This alarm may also occur and clear when the DHEI cable, the SWIF cable, or the DVB ASI cable is disconnected and then reconnected.

This alarm is self-clearing and may be intermittent due to random noise in the system. Single instances of this alarm that clear automatically and that do not reappear are not a cause for concern.

Front Panel Message

Continuity Count Error

Possible Cause(s)

A cable is loose, disconnected, or defective.

There are data errors on the satellite link.

The rate of change of the IEC exceeds the allowed threshold.

There is defective upstream equipment or failure on the input data link of the QAM modulator.

There is defective local MPEG coding.

The QAM modulator is defective.

Check and Correct

Loose, disconnected, or defective cables

Check for loose connections or defective cables, tighten any loose cable connections, connect any disconnected cables, and replace any defective cables.

Chapter 1 QAM Modulator Alarms

Satellite link data errors

Contact your signal provider to verify if there are any problems with their satellite transmissions.

IEC errors

Clean up the MPEG signal input to the QAM modulator by checking the IRT, RTE, and MPEG encoder.

Defective upstream equipment

- 1 Check the upstream devices that are sending MPEG packets to the QAM modulator.

Important!

- If the majority of MPEG packet alarms are occurring in a single QAM modulator, then that QAM modulator or its input should be the focus of the troubleshooting.
 - If the majority of MPEG packet alarms are occurring in more than one QAM modulator, then the troubleshooting should focus upstream on the device that is providing a common source of input to the QAM modulators with errors.
 - If the QAM modulators all have a common device upstream, then that device is the most likely source of the packet errors
- 2 Run the Doctor Report on the DNCS, and examine the report for any network connectivity issues or indications of loss of service.
 - 3 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
 - 4 If the alarm continues to occur, contact Cisco Services for further assistance.

Defective local MPEG coding

Check the local source devices that are providing MPEG content to the QAM modulator.

QAM modulator defective

- 1 Replace the QAM modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the QAM modulator.
- 2 If the alarm continues to occur, contact Cisco Services for further assistance.

QAM Modulator Alarm ID 22 (16 Hex)

The **Transport Error** alarm occurs when the QAM modulator detects a TEI error. There is a potential for loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the QAM modulator that is sending this alarm.

Front Panel Message

TBD

Possible Cause(s)

There is an error in the header of the MPEG packet.

Check and Correct

- 1 Replace the QAM modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the QAM modulator.
- 2 If the alarm continues to occur, contact Cisco Services for further assistance.

QAM Modulator Alarm ID 23 (17 Hex)

The **Control Word Server Error** alarm occurs when the QAM modulator cannot obtain proper control words from the Control Word server. This results in a loss of video on some DHCTs. There is a potential for loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the QAM modulator that is sending this alarm.

Front Panel Message

TBD

Possible Cause(s)

- There are errors in the configuration of the Control Word server.
- There is communication failure in the Ethernet link from the QAM modulator to the Control Word server.

Check and Correct

Configuration errors

Verify proper configuration of the Control Word server.

Ethernet link failure

- 1 Verify proper Ethernet connection and configuration.
- 2 If the alarm continues to occur, contact Cisco Services for further assistance.

QAM Modulator Alarm ID 24 (18 Hex)

The **ECM Bandwidth Error** alarm occurs when there is not enough channel capacity in the downstream QAM modulator path to insert PowerKEY® ECMs. If this QAM modulator is carrying encrypted video content, failure to deliver ECMs will result in black screens, flashing video, poor video quality, and other degradations to service.

Front Panel Message

TBD

Possible Cause(s)

The input data stream has too much data, and not enough MPEG null packets for proper QAM modulator operation.

Check and Correct

- 1 Reduce the number of services on the multiplexer (BitMizer™, Cherry Picker, etc.) until more channel capacity can be obtained from the program provider.
- 2 Move one of the program services to another QAM modulator.
- 3 Replace the QAM modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the QAM modulator.
- 4 If the alarm continues to occur, contact Cisco Services for further assistance.

QAM Modulator Alarm ID 25 (19 Hex)

The **ECM Not Found Error** alarm occurs when the QAM modulator cannot locate a CA descriptor for PowerKEY® ECMs in the input stream. If this QAM modulator is carrying encrypted video content, failure to deliver ECMs can cause black screens, flashing video, poor video quality, and other degradations to service.

Front Panel Message

TBD

Possible Cause(s)

The input data stream is not formatted properly.

Check and Correct

- 1 Verify the configuration of the MPEG source for proper settings.
- 2 If the alarm continues to occur, contact Cisco Services for further assistance.

QAM Modulator Alarm ID 26 (1A Hex)

The **Continuity Counter Error** alarm occurs when the QAM modulator detects continuity counter errors on the data input. The continuity counter error indicates an MPEG packet sequence problem, usually caused by dropped MPEG transport packets. There is potential loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the QAM modulator that is sending this alarm.

Front Panel Message

Continuity Count Error

Possible Cause(s)

- A cable is loose, disconnected, or defective.
- There are data errors on the satellite link.
- There is an error with the device(s) that is sending MPEG data to the QAM modulator.

Check and Correct

Loose, disconnected, or defective cables

Check for loose connections or defective cables, tighten any loose cable connections, connect any disconnected cables, and replace any defective cables.

Satellite link data errors

Contact your signal provider and verify proper operation of the satellite link.

MPEG data device error

- 1 Verify proper operation of the device sending data to the QAM modulator.
- 2 Run the Doctor Report on the DNCS, and examine the report for any network connectivity issues or indications of loss of services.
- 3 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report. If you cannot resolve these issues, contact Cisco Services.

QAM Modulator Alarm ID 27 (1B Hex)

The **Transport Error Indicator Error** alarm occurs when the QAM modulator receives MPEG packets with the TEI bit set to one. The TEI error also occurs when the equipment located upstream from the QAM modulator detects transmission errors. There is potential loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the QAM modulator that is sending this alarm.

Front Panel Message

Errored MPEG packets

Possible Cause(s)

- A cable is loose, disconnected, or defective.
- There are data errors on the satellite link.
- There is an error with the device(s) that is sending MPEG data to the QAM modulator.

Check and Correct

Loose, disconnected, or defective cables

Check for loose connections or defective cables, tighten any loose cable connections, connect any disconnected cables, and replace any defective cables.

Satellite link data errors

Contact your signal provider and verify proper operation of the satellite link.

MPEG data device error

- 1 Verify proper operation of the device sending data to the QAM modulator.
- 2 Run the Doctor Report on the DNCS, and examine the report for any network connectivity issues or indications of loss of services.
- 3 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report. If you cannot resolve these issues, contact Cisco Services.

2

MQAM Modulator Alarms

Introduction

This chapter provides detailed information for troubleshooting the alarms that are generated by the MQAM modulator. The alarms are arranged in the ascending numeric order of the Alarm IDs. For your convenience, the Alarm IDs are listed in both decimal and hexadecimal format. You can look up the possible causes and then follow the check and correct procedures for each alarm to help you troubleshoot and clear each alarm.

MQAM Modulator Alarm ID 1 (1 Hex)

The **RF1 Communication Error** alarm occurs when the digital I/O board in the MQAM modulator cannot communicate with the RF MCU at RF OUT 1. When this alarm occurs, video is not transmitted through the RF OUT 1 port.

Front Panel Message

RF1 Comm. failure

Possible Cause(s)

- The digital I/O board cannot communicate with the MCU on the MQAM modulator RF board at RF OUT 1.
- The MCU at RF OUT 1 on the MQAM modulator is not programmed correctly.
- The CRC checksum error did not clear correctly.
- The power supply failed or is failing.

Check and Correct

Digital I/O board cannot communicate with the MCU

Check for loose connections or defective cables, tighten any loose cables, and replace any defective cables.

MCU not programmed correctly

- 1 Power down and then power up the MQAM modulator using the on/off rocker-type switch on the back panel, or reset the MQAM modulator from the EC.
- 2 If resetting the MQAM modulator does not correct the problem, contact Cisco Broadband Services.

CRC checksum error

CRC errors are transient and intermittent and clear automatically.

Power supply failure

Replace the MQAM modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the MQAM modulator.

MQAM Modulator Alarm ID 2 (2 Hex)

The **RF1 Excessive Temperature** alarm occurs when the internal temperature of the MQAM modulator exceeds 70°C (158°F). An MQAM modulator that is overheating could have minimal to severe impact on services. If the modulator fails due to overheating, there would be no services available from that MQAM modulator.

Front Panel Message

RF1 Exceeded max temp

Possible Cause(s)

- The vents on the MQAM modulator are blocked.
- The room temperature is too high.
- A fan failure occurred.
- A hardware failure occurred.

Check and Correct

Vents are blocked

Check and clear any obstructions from the vents.

Room temperature is too high

Check and repair or replace the heating/cooling equipment in the room.

Fan failure

Check and repair or replace the fan.

Hardware failure

- 1 Replace the MQAM modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the MQAM modulator.
- 2 If the alarm condition continues to occur, contact Cisco Broadband Services.

MQAM Modulator Alarm ID 3 (3 Hex)

The **RF1 Power Supply Failure** alarm occurs when at least one internal power supply in the MQAM modulator fails. There is no RF output at RF OUT 1 when this condition exists, and video is not transmitted through the RF OUT 1 port. This condition could also generate a communication alarm. No services are available through the RF OUT 1 port.

Front Panel Message

RF1 Power supply failure

Possible Cause(s)

The internal power supply to RF OUT 1 in the MQAM modulator has failed or is failing.

Note: The RF output field on the front panel LCD screen displays “MUTED” when this condition exists.

Check and Correct

- 1 Check power source, power wires, and the on/off rocker-type switch on the back panel of the MQAM modulator.
- 2 Replace the MQAM modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the MQAM modulator.
- 3 Contact Cisco Broadband Services for further assistance.

MQAM Modulator Alarm ID 4 (4 Hex)

The **RF1 DC Lock Detect Error** alarm occurs when the DC lock detect signal at RF OUT 1 in the MQAM modulator is functioning incorrectly. There is no RF output at RF OUT 1 when this condition exists, and video is not transmitted through the RF OUT 1 port.

Front Panel Message

RF1 DC Lock detect error

Possible Cause(s)

- The DC lock detect signal at RF OUT 1 in the MQAM modulator is functioning incorrectly.
- During the MCU POST, the lock detect signal from the DC PLL at RF OUT 1 in the MQAM modulator did not indicate an unlocked condition when one existed.
- The output converter synthesizer in the MQAM modulator has malfunctioned.
Note: The RF output field on the front panel LCD screen displays “MUTED” when this condition exists.

Check and Correct

- 1 Power down and then power up the MQAM modulator using the on/off rocker-type switch on the back panel, or reset the MQAM modulator from the DNCS.
- 2 Replace the MQAM modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the MQAM modulator.
- 3 Contact Cisco Services for further assistance.

MQAM Modulator Alarm ID 5 (5 Hex)

The **RF1 DC PLL Unlocked Error** alarm occurs when the DC PLL synthesizer at RF OUT 1 in the MQAM modulator cannot lock. There is no RF output at RF OUT 1 when this condition exists because the signal is not synchronized, and video is not transmitted through the RF OUT 1 port.

Front Panel Message

RF1 DC PLL unlocked

Possible Cause(s)

- The DC PLL synthesizer at RF OUT 1 in the MQAM modulator cannot lock.
- The output frequency in the MQAM modulator may be incorrect.

Note: The RF output field on the front panel LCD screen displays “MUTED” when this condition exists.

Check and Correct

The PLL synthesizer cannot lock or the output frequency is not correct

- 1 Power down and then power up the MQAM modulator using the on/off rocker-type switch on the back panel, or reset the MQAM modulator from the EC.
- 2 Replace the MQAM modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the MQAM modulator.
- 3 Contact Cisco Services for further assistance.

MQAM Modulator Alarm ID 6 (6 Hex)

The **RF1 ASIC Initialization Error** alarm occurs when the MCU at RF OUT 1 in the MQAM modulator cannot communicate with the ASIC during initialization. No services are available through the RF OUT 1 port.

Front Panel Message

RF1 ASIC init failure

Possible Cause(s)

The MCU at RF OUT 1 in the MQAM modulator could not communicate with the ASIC during initialization.

Check and Correct

- 1 Power down and then power up the MQAM modulator using the on/off rocker-type switch on the back panel, or reset the MQAM modulator from the EC.
- 2 Replace the MQAM modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the MQAM modulator.
- 3 If the alarm continues to occur, contact Cisco Services for further assistance.

MQAM Modulator Alarm ID 7 (7 Hex)

The **RF1 Calibration Error** alarm occurs when the RF level settings at RF OUT 1 in the MQAM modulator are not calibrated to the correct frequency, or when the EEPROM that stores the calibration data is not operational. When this condition exists, there is potential loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the MQAM modulator that is sending this alarm.

Front Panel Message

RF1 Level not calibrated

Possible Cause(s)

- The RF level settings at RF OUT 1 in the MQAM modulator are not calibrated to the correct frequency.
- The EEPROM that stores the calibration data for the MQAM modulator is not operational.

Check and Correct

- 1 Power down and then power up the MQAM modulator using the on/off rocker-type switch on the back panel, or reset the MQAM modulator from the EC.
- 2 Replace the MQAM modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the MQAM modulator.
- 3 If the alarm continues to occur, contact Cisco Services for further assistance.

MQAM Modulator Alarm ID 8 (8 Hex)

The **RF1 UC Lock Detect Error** alarm occurs when the UC PLL lock detect signal at RF OUT 1 in the MQAM modulator is functioning incorrectly. There is no RF output at RF OUT 1 when this condition exists, and therefore no services are available through the RF OUT 1 port.

Front Panel Message

RF1 UC Lock detect error

Possible Cause(s)

The UC PLL lock detect signal at RF OUT 1 in the MQAM modulator is functioning incorrectly.

Note: The RF output field on the front panel screen displays “MUTED” when this condition exists.

Check and Correct

- 1 Power down and then power up the MQAM modulator using the on/off rocker-type switch on the back panel, or reset the MQAM modulator from the EC.
- 2 If resetting the MQAM modulator does not solve the problem, contact Cisco Services for further assistance.

MQAM Modulator Alarm ID 9 (9 Hex)

The **RF1 UC PLL Unlocked Error** alarm occurs when the UC PLL at RF OUT 1 in the MQAM modulator is unlocked. There is no RF output at RF OUT 1 when this condition exists, and therefore no services are available through the RF OUT 1 port.

Front Panel Message

RF1 UC PLL unlocked

Possible Cause(s)

- The UC PLL at RF OUT 1 in the MQAM modulator is unlocked.
- The output frequency transmitted from the MQAM modulator may be incorrect.
Note: The RF output field on the front panel screen displays “MUTED” when this condition exists.

Check and Correct

- 1 Power down and then power up the MQAM modulator using the on/off rocker-type switch on the back panel, or reset the MQAM modulator from the EC.
- 2 If resetting the MQAM modulator does not solve the problem, contact Cisco Services for further assistance.

MQAM Modulator Alarm ID 10 (A Hex)

The **RF1 EEPROM Failure** alarm occurs when the EEPROM at RF OUT 1 in the MQAM modulator is not present or is not operational. No services or poor quality services are available through the RF OUT 1 port.

The following conditions also exist when this alarm occurs:

- RF calibration data is not available.
- The **MQAM Modulator RF (1-4) Calibration Error** alarm is active.
- The **RF (1-4) Level not calibrated** alarm message appears on the front panel LCD screen.

Front Panel Message

RF1 EEPROM failure

Possible Cause(s)

The EEPROM in the MQAM modulator at RF OUT 1 failed, is not present, or is not operational.

Check and Correct

- 1 Power down and then power up the MQAM modulator using the on/off rocker-type switch on the back panel, or reset the MQAM modulator from the EC.
- 2 Replace the MQAM modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the MQAM modulator.
- 3 Contact Cisco Services for further assistance.

MQAM Modulator Alarm ID 11 (B Hex)

The **RF1 Output Load Error** alarm occurs when the MCU at RF OUT 1 in the MQAM modulator detects a large amount of reflected RF power. This RF power overload indicates that the RF load impedance at the output is incorrect. No services or poor quality services are available through the RF OUT 1 port.

Front Panel Message

RF1 Output load error

Possible Cause(s)

A disconnected RF output cable, a loose RF output cable, or an RF output cable that is defective usually causes this condition.

Check and Correct

- 1 Check and tighten the RF cable connections, connect any disconnected cables, and then repair or replace any defective cables that are connected to the RF OUT 1 port on the back panel of the MQAM modulator.
- 2 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 3 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 4 If you cannot resolve the issues identified in the Doctor Report, contact Cisco Services.

MQAM Modulator Alarm ID 13 (D Hex)

The **RF2 Communication Error** alarm occurs when the digital I/O board in the MQAM modulator cannot communicate with the RF MCU at RF OUT 2. When this alarm occurs, video is not transmitted through the RF OUT 2 port.

Front Panel Message

RF2 Comm. failure

Possible Cause(s)

- The digital I/O board cannot communicate with the MCU on the MQAM modulator RF board at RF OUT 2. This could be caused by loose or defective cables.
- The MCU at RF OUT 2 on the MQAM modulator is not programmed correctly.
- The CRC checksum error did not clear correctly.
- The power supply failed or is failing.

Check and Correct

Digital I/O board cannot communicate with the MCU

Check for loose connections or defective cables, tighten any loose cables, connect any disconnected cables, and replace any defective cables.

MCU not programmed correctly

- 1 Power down and then power up the MQAM modulator using the on/off rocker-type switch on the back panel, or reset the MQAM modulator from the EC.
- 2 If resetting the MQAM modulator does not correct the problem, contact Cisco Services.

CRC checksum error

CRC errors are transient and intermittent and clear automatically.

Power supply failure

Replace the MQAM modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the MQAM modulator.

MQAM Modulator Alarm ID 14 (E Hex)

The **RF2 Excessive Temperature** alarm occurs when the internal temperature of the MQAM modulator exceeds 70°C (158°F). An MQAM modulator that is overheating could have minimal to severe impact on services. If the modulator fails due to overheating, there would be no services available from that MQAM modulator.

Front Panel Message

RF2 Exceeded max temp

Possible Cause(s)

- The vents on the MQAM modulator are blocked.
- The room temperature is too high.
- A fan failure occurred.
- A hardware failure occurred.

Check and Correct

Vents are blocked

Check and clear any obstructions from the vents.

Room temperature is too high

Check and repair or replace the heating/cooling equipment in the room.

Fan failure

Check and repair or replace the fan.

Hardware failure

- 1 Replace the MQAM modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the MQAM modulator.
- 2 If the alarm condition continues to occur, contact Cisco Services.

MQAM Modulator Alarm ID 15 (F Hex)

The **RF2 Power Supply Failure** alarm occurs when at least one internal power supply in the MQAM modulator fails. There is no RF output at RF OUT 2 when this condition exists and video is not transmitted through the RF OUT 2 port. This condition could also generate a communication alarm.

Front Panel Message

RF2 Power supply failure

Possible Cause(s)

The internal power supply to RF OUT 2 in the MQAM modulator has failed or is failing.

Note: The RF output field on the front panel LCD screen displays “MUTED” when this condition exists.

Check and Correct

- 1 Check power source, power wires, and the on/off switch on the back panel of the MQAM modulator.
- 2 Replace the MQAM modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the MQAM modulator.
- 3 Contact Cisco Services for further assistance.

MQAM Modulator Alarm ID 16 (10 Hex)

The **RF2 DC Lock Detect Error** alarm occurs when the DC lock detect signal at RF OUT 2 in the MQAM modulator is functioning incorrectly. There is no RF output at RF OUT 2 when this condition exists, and video is not transmitted through the RF OUT 2 port.

Front Panel Message

RF2 DC Lock detect error

Possible Cause(s)

- The DC lock detect signal at RF OUT 2 in the MQAM modulator is functioning incorrectly.
- During the MCU POST, the lock detect signal from the DC PLL at RF OUT 2 in the MQAM modulator did not indicate an unlocked condition when one existed.
- The output converter synthesizer in the MQAM modulator has malfunctioned.
Note: The RF output field on the front panel LCD screen displays “MUTED” when this condition exists.

Check and Correct

- 1 Power down and then power up the MQAM modulator using the on/off rocker-type switch on the back panel, or reset the MQAM modulator from the EC.
- 2 Replace the MQAM modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the MQAM modulator.
- 3 Contact Cisco Services for further assistance.

MQAM Modulator Alarm ID 17 (11 Hex)

The **RF2 DC PLL Unlocked Error** alarm occurs when the DC PLL synthesizer at RF OUT 2 in the MQAM modulator cannot lock. There is no RF output at RF OUT 2 when this condition exists because the signal is not synchronized, and video is not transmitted through the RF OUT 2 port.

Front Panel Message

RF2 DC PLL unlocked

Possible Cause(s)

- The DC PLL synthesizer at RF OUT 2 in the MQAM modulator cannot lock.
- The output frequency in the MQAM modulator may be incorrect.

Note: The RF output field on the front panel LCD screen displays “MUTED” when this condition exists.

Check and Correct

- 1 Power down and then power up the MQAM modulator using the on/off rocker-type switch on the back panel, or reset the MQAM modulator from the EC.
- 2 Replace the MQAM modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the MQAM modulator.
- 3 Contact Cisco Services for further assistance.

MQAM Modulator Alarm ID 18 (12 Hex)

The **RF2 ASIC Initialization Error** alarm occurs when the MCU at RF OUT 2 in the MQAM modulator cannot communicate with the ASIC during initialization. No services are available through the RF OUT 2 port.

Front Panel Message

RF2 ASIC init failure

Possible Cause(s)

The MCU at RF OUT 2 in the MQAM modulator could not communicate with the ASIC during initialization.

Check and Correct

- 1 Power down and then power up the MQAM modulator using the on/off rocker-type switch on the back panel, or reset the MQAM modulator from the EC.
- 2 Replace the MQAM modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the MQAM modulator.
- 3 Contact Cisco Services for further assistance.

MQAM Modulator Alarm ID 19 (13 Hex)

The **RF2 Calibration Error** alarm occurs when the RF level settings at RF OUT 2 in the MQAM modulator are not calibrated to the correct frequency, or when the EEPROM that stores the calibration data is not operational. There is potential loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the MQAM modulator that is sending this alarm.

Front Panel Message

RF2 Level not calibrated

Possible Cause(s)

- The RF level settings at RF OUT 2 in the MQAM modulator are not calibrated to the correct frequency.
- The EEPROM that stores the calibration data for the MQAM modulator is not operational.

Check and Correct

- 1 Power down and then power up the MQAM modulator using the on/off rocker-type switch on the back panel, or reset the MQAM modulator from the EC.
- 2 Replace the MQAM modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the MQAM modulator.
- 3 Contact Cisco Services for further assistance.

MQAM Modulator Alarm ID 20 (14 Hex)

The **RF2 UC Lock Detect Error** alarm occurs when the UC PLL lock detect signal at RF OUT 2 in the MQAM modulator is functioning incorrectly. There is no RF output at RF OUT 2 when this condition exists, and therefore no services are available through the RF OUT 2 port.

Front Panel Message

RF2 UC Lock detect error

Possible Cause(s)

The UC PLL lock detect signal at RF OUT 2 in the MQAM modulator is functioning incorrectly.

Note: The RF output field on the front panel screen displays “MUTED” when this condition exists.

Check and Correct

- 1 Power down and then power up the MQAM modulator using the on/off rocker-type switch on the back panel, or reset the MQAM modulator from the EC.
- 2 Contact Cisco Services for further assistance.

MQAM Modulator Alarm ID 21 (15 Hex)

The **RF2 UC PLL Unlocked Error** alarm occurs when the UC PLL at RF OUT 2 in the MQAM modulator is unlocked. There is no RF output at RF OUT 2 when this condition exists, and therefore no services are available through the RF OUT 2 port.

Front Panel Message

RF2 UC PLL unlocked

Possible Cause(s)

- The UC PLL at RF OUT 2 in the MQAM modulator is unlocked.
- The output frequency transmitted from the MQAM modulator may be incorrect.
Note: The RF output field on the front panel screen displays “MUTED” when this condition exists.

Check and Correct

- 1 Power down and then power up the MQAM modulator using the on/off rocker-type switch on the back panel, or reset the MQAM modulator from the EC.
- 2 Contact Cisco Services for further assistance.

MQAM Modulator Alarm ID 22 (16 Hex)

The **RF2 EEPROM Failure** alarm occurs when the EEPROM at RF OUT 2 in the MQAM modulator is not present or is not operational. No services or poor quality services are available through the RF OUT 2 port.

The following conditions also exist when this alarm occurs:

- RF calibration data is not available.
- The **MQAM Modulator RF (1-4) Calibration Error** alarm is active.
- The **RF (1-4) Level not calibrated** alarm message appears on the front panel LCD screen.

Front Panel Message

RF2 EEPROM failure

Possible Cause(s)

The EEPROM in the MQAM modulator at RF OUT 2 failed, is not present, or is not operational.

Check and Correct

- 1 Power down and then power up the MQAM modulator using the on/off rocker-type switch on the back panel, or reset the MQAM modulator from the EC.
- 2 Replace the MQAM modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the MQAM modulator.
- 3 Contact Cisco Services for further assistance.

MQAM Modulator Alarm ID 23 (17 Hex)

The **RF2 Output Load Error** alarm occurs when the MCU at RF OUT 2 in the MQAM modulator detects a large amount of reflected RF power. This RF power overload indicates that the RF load impedance at the output is incorrect. No services or poor quality services are available through the RF OUT 2 port.

Front Panel Message

RF2 Output load error

Possible Cause(s)

A disconnected RF output cable, a loose RF output cable, or an RF output cable that is defective usually causes this condition.

Check and Correct

- 1 Check and tighten the RF cable connections, connect any disconnected cables, and then repair or replace any defective cables that are connected to the RF OUT 2 port on the back panel of the MQAM modulator.
- 2 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 3 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 4 If you cannot resolve the issues identified in the Doctor Report, contact Cisco Services.

MQAM Modulator Alarm ID 25 (19 Hex)

The **RF3 Communication Error** alarm occurs when the digital I/O board in the MQAM modulator cannot communicate with the RF MCU at RF OUT 3. When this alarm occurs, video is not transmitted through the RF OUT 3 port.

Front Panel Message

RF3 Comm. failure

Possible Cause(s)

- The digital I/O board cannot communicate with the MCU on the MQAM modulator RF board at RF OUT 3. This could be caused by loose or defective cables.
- The MCU at RF OUT 3 on the MQAM modulator is not programmed correctly.
- The CRC checksum error did not clear correctly.
- The power supply failed or is failing.

Check and Correct

Digital I/O board cannot communicate with the MCU

Check for loose connections or defective cables, tighten any loose cables, connect any disconnected cables, and replace any defective cables.

MCU not programmed correctly

- 1 Power down and then power up the MQAM modulator using the on/off rocker-type switch on the back panel, or reset the MQAM modulator from the EC.
- 2 If resetting the MQAM modulator does not correct the problem, contact Cisco Services.

CRC checksum error

CRC errors are transient and intermittent and clear automatically.

Power supply failure

Replace the MQAM modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the MQAM modulator.

MQAM Modulator Alarm ID 26 (1A Hex)

The **RF3 Excessive Temperature** alarm occurs when the internal temperature of the MQAM modulator exceeds 70°C (158°F). An MQAM modulator that is overheating could have minimal to severe impact on services. If the modulator fails due to overheating, there would be no services available from that MQAM modulator.

Front Panel Message

RF3 Exceeded max temp

Possible Cause(s)

- The vents on the MQAM modulator are blocked.
- The room temperature is too high.
- A fan failure occurred.
- A hardware failure occurred.

Check and Correct

Vents are blocked

Check and clear any obstructions from the vents.

Room temperature is too high

Check and repair or replace the heating/cooling equipment in the room.

Fan failure

Check and repair or replace the fan.

Hardware failure

- 1 Replace the MQAM modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the MQAM modulator.
- 2 If the alarm condition continues to occur, contact Cisco Services.

MQAM Modulator Alarm ID 27 (1B Hex)

The **RF3 Power Supply Failure** alarm occurs when at least one internal power supply in the MQAM modulator fails. There is no RF output at RF OUT 3 when this condition exists and video is not transmitted through the RF OUT 3 port. This condition could also generate a communication alarm.

Front Panel Message

RF3 Power supply failure

Possible Cause(s)

The internal power supply to RF OUT 3 in the MQAM modulator has failed or is failing.

Note: The RF output field on the front panel LCD screen displays “MUTED” when this condition exists.

Check and Correct

- 1 Check power source, power wires, and the on/off rocker-type switch on the back panel of the MQAM modulator.
- 2 Replace the MQAM modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the MQAM modulator.
- 3 Contact Cisco Services for further assistance.

MQAM Modulator Alarm ID 28 (1C Hex)

The **RF3 DC Lock Detect Error** alarm occurs when the DC lock detect signal at RF OUT 3 in the MQAM modulator is functioning incorrectly. There is no RF output at RF OUT 3 when this condition exists, and video is not transmitted through the RF OUT 3 port.

Front Panel Message

RF3 DC Lock detect error

Possible Cause(s)

- The DC lock detect signal at RF OUT 3 in the MQAM modulator is functioning incorrectly.
- During the MCU POST, the lock detect signal from the DC PLL at RF OUT 3 in the MQAM modulator did not indicate an unlocked condition when one existed.
- The output converter synthesizer in the MQAM modulator has malfunctioned.
Note: The RF output field on the front panel LCD screen displays “MUTED” when this condition exists.

Check and Correct

- 1 Power down and then power up the MQAM modulator using the on/off rocker-type switch on the back panel, or reset the MQAM modulator from the EC.
- 2 Replace the MQAM modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the MQAM modulator.
- 3 Contact Cisco Services for further assistance.

MQAM Modulator Alarm ID 29 (1D Hex)

The **RF3 DC PLL Unlocked Error** alarm occurs when the DC PLL synthesizer at RF OUT 3 in the MQAM modulator cannot lock. There is no RF output at RF OUT 3 when this condition exists because the signal is not synchronized, and video is not transmitted through the RF OUT 3 port.

Front Panel Message

RF3 DC PLL unlocked

Possible Cause(s)

- The DC PLL synthesizer at RF OUT 3 in the MQAM modulator cannot lock.
- The output frequency in the MQAM modulator may be incorrect.

Note: The RF output field on the front panel LCD screen displays “MUTED” when this condition exists.

Check and Correct

- 1 Power down and then power up the MQAM modulator using the on/off rocker-type switch on the back panel, or reset the MQAM modulator from the EC.
- 2 Replace the MQAM modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the MQAM modulator.
- 3 Contact Cisco Services for further assistance.

MQAM Modulator Alarm ID 30 (1E Hex)

The **RF3 ASIC Initialization Error** alarm occurs when the MCU at RF OUT 3 in the MQAM modulator cannot communicate with the ASIC during initialization. No services are available through the RF OUT 3 port.

Front Panel Message

RF3 ASIC init failure

Possible Cause(s)

The MCU at RF OUT 3 in the MQAM modulator could not communicate with the ASIC during initialization.

Check and Correct

- 1 Power down and then power up the MQAM modulator using the on/off rocker-type switch on the back panel, or reset the MQAM modulator from the EC.
- 2 Replace the MQAM modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the MQAM modulator.
- 3 Contact Cisco Services for further assistance.

MQAM Modulator Alarm ID 31 (1F Hex)

The **RF3 Calibration Error** alarm occurs when the RF level settings at RF OUT 3 in the MQAM modulator are not calibrated to the correct frequency, or when the EEPROM that stores the calibration data is not operational. There is potential loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the MQAM modulator that is sending this alarm.

Front Panel Message

RF3 Level not calibrated

Possible Cause(s)

- The RF level settings at RF OUT 3 in the MQAM modulator are not calibrated to the correct frequency.
- The EEPROM that stores the calibration data for the MQAM modulator is not operational.

Check and Correct

- 1 Power down and then power up the MQAM modulator using the on/off rocker-type switch on the back panel, or reset the MQAM modulator from the EC.
- 2 Replace the MQAM modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the MQAM modulator.
- 3 Contact Cisco Services for further assistance.

MQAM Modulator Alarm ID 32 (20 Hex)

The **RF3 UC Lock Detect Error** alarm occurs when the UC PLL lock detect signal at RF OUT 3 in the MQAM modulator is functioning incorrectly. There is no RF output at RF OUT 3 when this condition exists, and therefore no services are available through the RF OUT 3 port.

Front Panel Message

RF3 UC Lock detect error

Possible Cause(s)

The UC PLL lock detect signal at RF OUT 3 in the MQAM modulator is functioning incorrectly.

Note: The RF output field on the front panel screen displays “MUTED” when this condition exists.

Check and Correct

- 1 Power down and then power up the MQAM modulator using the on/off rocker-type switch on the back panel, or reset the MQAM modulator from the EC.
- 2 If resetting the MQAM modulator does not solve the problem, contact Cisco Services for further assistance.

MQAM Modulator Alarm ID 33 (21 Hex)

The **RF3 UC PLL Unlocked Error** alarm occurs when the UC PLL at RF OUT 3 in the MQAM modulator is unlocked. There is no RF output at RF OUT 3 when this condition exists, and therefore no services are available through the RF OUT 3 port.

Front Panel Message

RF3 UC PLL unlocked

Possible Cause(s)

- The UC PLL at RF OUT 3 in the MQAM modulator is unlocked.
- The output frequency transmitted from the MQAM modulator may be incorrect.
Note: The RF output field on the front panel screen displays “MUTED” when this condition exists.

Check and Correct

- 1 Power down and then power up the MQAM modulator using the on/off rocker-type switch on the back panel, or reset the MQAM modulator from the EC.
- 2 If resetting the MQAM modulator does not solve the problem, contact Cisco Services for further assistance.

MQAM Modulator Alarm ID 34 (22 Hex)

The **RF3 EEPROM Failure** alarm occurs when the EEPROM at RF OUT 3 in the MQAM modulator is not present or is not operational. No services or poor quality services are available through the RF OUT 3 port.

The following conditions also exist when this alarm occurs:

- RF calibration data is not available.
- The **MQAM Modulator RF (1-4) Calibration Error** alarm is active.
- The **RF (1-4) Level not calibrated** alarm message appears on the front panel LCD screen.

Front Panel Message

RF3 EEPROM failure

Possible Cause(s)

The EEPROM in the MQAM modulator at RF OUT 3 failed, is not present, or is not operational.

Check and Correct

- 1 Power down and then power up the MQAM modulator using the on/off rocker-type switch on the back panel, or reset the MQAM modulator from the EC.
- 2 Replace the MQAM modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the MQAM modulator.
- 3 Contact Cisco Services for further assistance.

MQAM Modulator Alarm ID 35 (23 Hex)

The **RF3 Output Load Error** alarm occurs when the MCU at RF OUT 3 in the MQAM modulator detects a large amount of reflected RF power. This RF power overload indicates that the RF load impedance at the output is incorrect. No services or poor quality services are available through the RF OUT 3 port.

Front Panel Message

RF3 Output load error

Possible Cause(s)

A disconnected RF output cable, a loose RF output cable, or an RF output cable that is defective usually causes this condition.

Check and Correct

- 1 Check and tighten the RF cable connections, connect any disconnected cables, and then repair or replace any defective cables that are connected to the RF OUT 3 port on the back panel of the MQAM modulator.
- 2 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services. Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 3 If you cannot resolve the issues identified in the Doctor Report, contact Cisco Services.

MQAM Modulator Alarm ID 37 (25 Hex)

The **RF4 Communication Error** alarm occurs when the digital I/O board in the MQAM modulator cannot communicate with the RF MCU at RF OUT 4. When this alarm occurs, video is not transmitted through the RF OUT 4 port.

Front Panel Message

RF4 Comm. failure

Possible Cause(s)

- The digital I/O board cannot communicate with the MCU on the MQAM modulator RF board at RF OUT 4. This could be caused by loose or defective cables.
- The MCU at RF OUT 4 on the MQAM modulator is not programmed correctly.
- The CRC checksum error did not clear correctly.
- The power supply failed or is failing.

Check and Correct

Digital I/O board cannot communicate with the MCU

Check for loose connections or defective cables, tighten any loose cables, connect any disconnected cables, and replace any defective cables.

MCU not programmed correctly

- 1 Power down and then power up the MQAM modulator using the on/off rocker-type switch on the back panel, or reset the MQAM modulator from the EC.
- 2 If resetting the MQAM modulator does not solve the problem, contact Cisco Services.

CRC checksum error

CRC errors are transient and intermittent and clear automatically.

Power supply failure

Replace the MQAM modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the MQAM modulator.

MQAM Modulator Alarm ID 38 (26 Hex)

The **RF4 Excessive Temperature** alarm occurs when the internal temperature of the MQAM modulator exceeds 70°C (158°F). An MQAM modulator that is overheating could have minimal to severe impact on services. If the modulator fails due to overheating, there would be no services available from that MQAM modulator.

Front Panel Message

RF4 Exceeded max temp

Possible Cause(s)

- The vents on the MQAM modulator are blocked.
- The room temperature is too high.
- A fan failure occurred.
- A hardware failure occurred.

Check and Correct

Vents are blocked

Check and clear any obstructions from the vents.

Room temperature is too high

Check and repair or replace the heating/cooling equipment in the room.

Fan failure

Check and repair or replace the fan.

Hardware failure

- 1 Replace the MQAM modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the MQAM modulator.
- 2 If the alarm condition continues to occur, contact Cisco Services.

MQAM Modulator Alarm ID 39 (27 Hex)

The **RF4 Power Supply Failure** alarm occurs when at least one internal power supply in the MQAM modulator fails. There is no RF output at RF OUT 4 when this condition exists and video is not transmitted through the RF OUT 4 port. This condition could also generate a communication alarm.

Front Panel Message

RF4 Power supply failure

Possible Cause(s)

The internal power supply to RF OUT 4 in the MQAM modulator has failed or is failing.

Note: The RF output field on the front panel LCD screen displays “MUTED” when this condition exists.

Check and Correct

- 1 Check power source, power wires, and the on/off switch on the back panel of the MQAM modulator.
- 2 Replace the MQAM modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the MQAM modulator.
- 3 Contact Cisco Services for further assistance.

MQAM Modulator Alarm ID 40 (28 Hex)

The **RF4 DC Lock Detect Error** alarm occurs when the DC lock detect signal at RF OUT 4 in the MQAM modulator is functioning incorrectly. There is no RF output at RF OUT 4 when this condition exists, and video is not transmitted through the RF OUT 4 port.

Front Panel Message

RF4 DC Lock detect error

Possible Cause(s)

- The DC lock detect signal at RF OUT 4 in the MQAM modulator is functioning incorrectly.
- During the MCU POST, the lock detect signal from the DC PLL at RF OUT 4 in the MQAM modulator did not indicate an unlocked condition when one existed.
- The output converter synthesizer in the MQAM modulator has malfunctioned.
Note: The RF output field on the front panel LCD screen displays “MUTED” when this condition exists.

Check and Correct

- 1 Power down and then power up the MQAM modulator using the on/off rocker-type switch on the back panel, or reset the MQAM Modulator from the EC.
- 2 Replace the MQAM modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the MQAM modulator.
- 3 Contact Cisco Services for further assistance.

MQAM Modulator Alarm ID 41 (29 Hex)

The **RF4 DC PLL Unlocked Error** alarm occurs when the DC PLL synthesizer at RF OUT 4 in the MQAM modulator cannot lock. There is no RF output at RF OUT 4 when this condition exists because the signal is not synchronized, and video is not transmitted through the RF OUT 4 port.

Front Panel Message

RF4 DC PLL unlocked

Possible Cause(s)

- The DC PLL synthesizer at RF OUT 4 in the MQAM modulator cannot lock.
- The output frequency in the MQAM modulator may be incorrect.

Note: The RF output field on the front panel LCD screen displays “MUTED” when this condition exists.

Check and Correct

- 1 Power down and then power up the MQAM modulator using the on/off rocker-type switch on the back panel, or reset the MQAM modulator from the EC.
- 2 Replace the MQAM modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the MQAM modulator.
- 3 Contact Cisco Services for further assistance.

MQAM Modulator Alarm ID 42 (2A Hex)

The **RF4 ASIC Initialization Error** alarm occurs when the MCU at RF OUT 4 in the MQAM modulator cannot communicate with the ASIC during initialization. No services are available through the RF OUT 4 port.

Front Panel Message

RF4 ASIC init failure

Possible Cause(s)

The MCU at RF OUT 4 in the MQAM modulator could not communicate with the ASIC during initialization.

Check and Correct

- 1 Power down and then power up the MQAM modulator using the on/off rocker-type switch on the back panel, or reset the MQAM modulator from the EC.
- 2 Replace the MQAM modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the MQAM modulator.
- 3 Contact Cisco Services for further assistance.

MQAM Modulator Alarm ID 43 (2B Hex)

The **RF4 Calibration Error** alarm occurs when the RF level settings at RF OUT 4 in the MQAM modulator are not calibrated to the correct frequency, or when the EEPROM that stores the calibration data is not operational. There is a potential for loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the MQAM modulator that is sending this alarm.

Front Panel Message

RF4 Level not calibrated

Possible Cause(s)

The RF level settings at RF OUT 4 in the MQAM modulator are not calibrated to the correct frequency.

The EEPROM that stores the calibration data for the MQAM modulator is not operational.

Check and Correct

- 1 Power down and then power up the MQAM modulator using the on/off rocker-type switch on the back panel, or reset the MQAM modulator from the EC.
- 2 Replace the MQAM modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the MQAM modulator.
- 3 Contact Cisco Services for further assistance.

MQAM Modulator Alarm ID 44 (2C Hex)

The **RF4 UC Lock Detect Error** alarm occurs when the UC PLL lock detect signal at RF OUT 4 in the MQAM modulator is functioning incorrectly. There is no RF output at RF OUT 4 when this condition exists, and therefore no services are available through the RF OUT 4 port.

Front Panel Message

RF4 UC Lock detect error

Possible Cause(s)

The UC PLL lock detect signal at RF OUT 4 in the MQAM modulator is functioning incorrectly.

Note: The RF output field on the front panel screen displays “MUTED” when this condition exists.

Check and Correct

- 1 Power down and then power up the MQAM modulator using the on/off rocker-type switch on the back panel, or reset the MQAM modulator from the EC.
- 2 If resetting the MQAM modulator does not solve the problem, contact Cisco Services for further assistance.

MQAM Modulator Alarm ID 45 (2D Hex)

The **RF4 UC PLL Unlocked Error** alarm occurs when the UC PLL at RF OUT 4 in the MQAM modulator is unlocked. There is no RF output at RF OUT 4 when this condition exists, and therefore no services are available through the RF OUT 4 port.

Front Panel Message

RF4 UC PLL unlocked

Possible Cause(s)

- The UC PLL at RF OUT 4 in the MQAM modulator is unlocked.
- The output frequency transmitted from the MQAM modulator may be incorrect.
Note: The RF output field on the front panel screen displays “MUTED” when this condition exists.

Check and Correct

- 1 Power down and then power up the MQAM modulator using the on/off rocker-type switch on the back panel, or reset the MQAM modulator from the EC.
- 2 If resetting the MQAM modulator does not solve the problem, contact Cisco Services for further assistance.

MQAM Modulator Alarm ID 46 (2E Hex)

The **RF4 EEPROM Failure** alarm occurs when the EEPROM at RF OUT 4 in the MQAM modulator is not present or is not operational. No services or poor quality services are available through the RF OUT 4 port.

The following conditions also exist when this alarm occurs:

- RF calibration data is not available.
- The **MQAM Modulator RF (1-4) Calibration Error** alarm is active.
- The **RF (1-4) Level not calibrated** alarm message appears on the front panel LCD screen.

Front Panel Message

RF4 EEPROM failure

Possible Cause(s)

The EEPROM in the MQAM modulator at RF OUT 4 failed, is not present, or is not operational.

Check and Correct

- 1 Power down and then power up the MQAM modulator using the on/off rocker-type switch on the back panel, or reset the MQAM modulator from the EC.
- 2 Replace the MQAM modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the MQAM modulator.
- 3 Contact Cisco Services for further assistance.

MQAM Modulator Alarm ID 47 (2F Hex)

The **RF4 Output Load Error** alarm occurs when the MCU at RF OUT 4 in the MQAM modulator detects a large amount of reflected RF power. This RF power overload indicates that the RF load impedance at the output is incorrect. No services or poor quality services are available through the RF OUT 4 port.

Front Panel Message

RF4 Output load error

Possible Cause(s)

A disconnected RF output cable, a loose RF output cable, or an RF output cable that is defective usually causes this condition.

Check and Correct

- 1 Check and tighten the RF cable connections, connect any disconnected cables, and then repair or replace any defective cables that are connected to the RF OUT 4 port on the back panel of the MQAM modulator.
- 2 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 3 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 4 If you cannot resolve the issues identified in the Doctor Report, contact Cisco Services.

MQAM Modulator Alarm ID 49 (31 Hex)

The **Reset Detected** status event occurs during the boot-up process, or when the MQAM modulator is reset by either a loss of power or a manual reset. There is a potential for loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the MQAM modulator that is sending this event until it returns for full service.

Front Panel Message

Reset detected

Possible Cause(s)

- The MQAM modulator is rebooting.
- A user or system operator reset the MQAM modulator.
- A loss of power occurred.
- There is a problem in the DBDS.

Check and Correct

Session and provisioning data are sent to the MQAM modulator again by the EC. However, you should also check the following:

- 1 Verify that there are still broadcast services on this MQAM modulator.
- 2 Verify that the reset did not adversely affect broadcast services.
- 3 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 4 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 5 Contact Cisco Services for further assistance.

MQAM Modulator Alarm ID 50 (32 Hex)

The **MPEG Continuity Error** alarm can occur when individual MPEG packets become corrupted due to random noise in the network. Each MPEG packet has a section for continuity bits that should contain a sequential value. These MPEG continuity bits are used by the MPEG packet recipient to verify that the packets in an MPEG stream are received in the correct sequential order and to verify that no packet loss has occurred.

This alarm also occurs when the MQAM modulator receives packets in the MPEG stream that do not contain MPEG continuity bits.

There is a potential for loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the MQAM modulator that is sending this alarm.

Notes:

- This alarm may also occur and clear when the DVB ASI cable is disconnected and then reconnected.
- This alarm is self-clearing and may be intermittent due to random noise in the system. Single instances of this alarm that clear automatically and that do not reappear are not a cause for concern.

Front Panel Message

MPEG Continuity Error

Possible Cause(s)

- A cable is loose, disconnected, or defective.
- There are data errors on the satellite link.
- The rate of change of the IEC exceeds the allowed threshold.
- There is defective upstream equipment or failure on the input data link of the MQAM modulator.
- There is defective local MPEG coding.
- The MQAM modulator is defective.

Check and Correct

Loose, disconnected, or defective cables

Check for loose connections or defective cables, tighten any loose cable connections, connect any disconnected cables, and replace any defective cables.

Chapter 2 MQAM Modulator Alarms

Satellite link data errors

Contact your signal provider to verify if there are any problems with their satellite transmissions.

IEC errors

Clean up the MPEG signal input to the MQAM modulator by checking the IRT, RTE, and MPEG encoder.

Defective upstream equipment

- 1 Check the upstream devices that are sending MPEG packets to the MQAM modulator.
- 2 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of service.

Important!

- If the majority of MPEG packet alarms are occurring in a single MQAM modulator, then that MQAM modulator or its input should be the focus of the troubleshooting.
 - If the majority of MPEG packet alarms are occurring in more than one MQAM modulator, then the troubleshooting should focus upstream on the device that is providing a common source of input to the MQAM modulators with errors.
 - If the MQAM modulators all have a common device upstream, then that device is the most likely source of the packet errors
- 3 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
 - 4 If the alarm continues to occur, contact Cisco Services for further assistance.

Defective local MPEG coding

Check the local source devices that are providing MPEG content to the MQAM modulator.

MQAM modulator defective

- 1 Replace the MQAM modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the MQAM modulator.
- 2 If the alarm continues to occur, contact Cisco Services for further assistance.

MQAM Modulator Alarm ID 51 (33 Hex)

The **MPEG Transport Error** alarm occurs when there is an error in the header of some of the MPEG packets received by the MQAM modulator. There is a potential for loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the MQAM modulator that is sending this alarm.

Note: This alarm is self-clearing and may be intermittent. Single instances of this alarm that clear automatically and that do not reappear are not a cause for concern.

Front Panel Message

MPEG Transport error

Possible Cause(s)

There is an error in the header of an MPEG packet.

Check and Correct

- 1 Check the upstream devices that are sending MPEG packets to the ASI input ports on the MQAM modulator.
- 2 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 3 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 4 If the alarm continues to occur, contact Cisco Services for further assistance.

MQAM Modulator Alarm ID 52 (34 Hex)

The **ASI1 Loss of Signal Error** alarm occurs when there is no ASI signal to the DVB ASI Input 1 port in the MQAM modulator. This alarm clears automatically when the DVB ASI Input 1 port is receiving valid data.

Front Panel Message

ASI1 Loss of input signal

Possible Cause(s)

- A cable is loose, disconnected, or defective.
- An upstream device providing input to the MQAM modulator failed or is offline.
- The MQAM modulator is defective.

Check and Correct

A cable is loose, disconnected, or defective

Check for loose cable connections or defective cables at the DVB ASI inputs on the back panel of the MQAM modulator, connect any disconnected cables, then tighten any loose cable connections, and replace any defective cables.

Upstream device failed or offline

- 1 Verify that the DVB ASI outputs of upstream devices are functioning correctly.
- 2 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 3 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 4 If the alarm continues to occur, contact Cisco Services for further assistance.

MQAM modulator is defective

- 1 Replace the MQAM modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the MQAM modulator.
- 2 Contact Cisco Services for further assistance.

MQAM Modulator Alarm ID 53 (35 Hex)

The **ASI1 MPEG Packets Error** alarm occurs when there are errors in the headers of the MPEG packets at the DVB ASI Input 1 port in the MQAM modulator. Errors include an invalid MPEG packet header where the first byte (for example, sync byte) is not equal to 47 Hex (0x47), or where the MPEG packet size is not exactly 188 bytes. There is a potential for loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the MQAM modulator that is sending this alarm.

This alarm may also occur when the DVB ASI cable is disconnected and then clear before you reconnect the cable. This clear occurs because the MPEG stream is disrupted and the device detects that the input signal is completely lost.

Note: This alarm is self-clearing and may be intermittent. Single instances of this alarm that clear automatically and that do not reappear are not a cause for concern.

Front Panel Message

ASI1 Errored MPEG packet

Possible Cause(s)

- A cable is loose, disconnected, or defective.
- There are data errors on the satellite link.
- The rate of change of the IEC exceeds the allowed threshold.
- Upstream devices that provide input to the MQAM modulator are sending errored MPEG packets.
- There is defective local MPEG coding.
- The MQAM modulator is defective.

Check and Correct

A cable is loose, disconnected, or defective

Check for loose connections or defective cables, tighten any loose cable connections, connect any disconnected cables, and replace any defective cables.

Note: This alarm may also occur when the DVB ASI cable is disconnected and then clear before you reconnect the cable. This is normal.

Data errors on the satellite link

Contact your signal provider to verify if there are any problems with their satellite transmissions.

Chapter 2 MQAM Modulator Alarms

IEC exceeds threshold

Clean up the MPEG signal input to the MQAM modulator by checking the IRT, RTE, and MPEG encoder.

Upstream devices sending errored MPEG packets

- 1 Check the upstream devices that are sending MPEG packets to the DVB ASI input ports on the MQAM modulator.
- 2 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 3 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 4 If the alarm continues to occur, contact Cisco Services for further assistance.

Defective local MPEG coding

Check the local source devices that are providing MPEG content to the MQAM modulator.

MQAM modulator is defective

- 1 Replace the MQAM modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the MQAM modulator.
- 2 Contact Cisco Services for further assistance.

MQAM Modulator Alarm ID 54 (36 Hex)

The **ASI1 FIFO Overflow Error** alarm occurs when there is a FIFO buffer overflow at the DVB ASI Input 1 port on the MQAM modulator, and packet data is lost. There is a potential for loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the MQAM modulator that is sending this alarm.

Note: This alarm is self-clearing and may be intermittent. Single instances of this alarm that clear automatically and that do not reappear are not a cause for concern.

Front Panel Message

ASI1 FIFO overflow

Possible Cause(s)

- The data rate as defined from the EC for the MQAM modulator sessions is too low, which also means that the data rate of the ASI input to the MQAM modulator is too high.
- There are too many sessions defined for the MQAM modulator from the EC.
- The modulation mode is incorrect.
- Upstream devices are sending too many MPEG packets to the MQAM modulator.
- A hardware problem occurred.

Check and Correct

Data rate too low

- 1 Reduce the amount of incoming data.
- 2 Reduce the amount of data added to the stream.
- 3 Increase the MQAM modulation mode.
- 4 Verify and correct session rate targets and threshold values.

Too many sessions defined

Reduce the total number of MPEG programs by deleting sessions.

Modulation mode incorrect

Verify and correct the modulation mode.

Upstream devices sending too many MPEG packets

Check the upstream devices that are sending MPEG packets to the DVB ASI input ports on the MQAM modulator.

Chapter 2 MQAM Modulator Alarms

Hardware problem

- 1 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 2 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 3 Replace the MQAM modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the MQAM modulator.
- 4 If the alarm continues to occur, contact Cisco Services for further assistance.

MQAM Modulator Alarm ID 55 (37 Hex)

The **ASI1 Excess Packets Dumped** alarm occurs when there is excessive bandwidth utilization on one or more channels at the DVB ASI Input 1 port on the MQAM modulator. Packets for those channels are being dumped so as not to affect the other channels.

There is potential loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the MQAM modulator that is sending this alarm.

Note: This alarm is self-clearing and may be intermittent. Single instances of this alarm that clear automatically and that do not reappear are not a cause for concern.

Front Panel Message

ASI1 Packets were dumped

Possible Cause(s)

- The data rate as defined from the EC for the MQAM modulator sessions is too low, which also means that the data rate of the ASI input to the MQAM modulator is too high.
- There are too many sessions defined for the MQAM modulator from the EC.
- The modulation mode is incorrect.
- Upstream devices are sending too many MPEG packets to the MQAM modulator.
- A hardware problem occurred.

Check and Correct

Data rate too low

- 1 Reduce the amount of incoming data.
- 2 Reduce the amount of data added to the stream.
- 3 Increase the MQAM modulation mode.
- 4 Verify and correct session rate targets and threshold values.

Too many sessions defined

Reduce the total number of MPEG programs by deleting sessions.

Modulation mode incorrect

Verify and correct the modulation mode.

Chapter 2 MQAM Modulator Alarms

Upstream devices sending too many MPEG packets

Check the upstream devices that are sending MPEG packets to the DVB ASI input ports on the MQAM modulator.

Hardware problem

- 1 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 2 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 3 Replace the MQAM modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the MQAM modulator.
- 4 If the alarm continues to occur, contact Cisco Services for further assistance.

MQAM Modulator Alarm ID 56 (38 Hex)

The **ASI2 Loss of Signal Error** alarm occurs when there is no ASI signal to the DVB ASI Input 2 port in the MQAM modulator. This alarm clears automatically when the DVB ASI Input 2 port is connected and is receiving valid data.

Front Panel Message

ASI2 Loss of input signal

Possible Cause(s)

- A cable is loose, disconnected, or defective.
- An upstream device providing input to the MQAM modulator failed or is offline.
- The MQAM modulator is defective.

Check and Correct

A cable is loose, disconnected, or defective

Check for loose cable connections or defective cables at the DVB ASI inputs on the back panel of the MQAM modulator, connect any disconnected cables, then tighten any loose cable connections, and replace any defective cables.

Upstream device failed or is offline

- 1 Verify that the DVB ASI outputs of upstream devices are functioning correctly.
- 2 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 3 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 4 If the alarm continues to occur, contact Cisco Services for further assistance

MQAM modulator is defective

- 1 Replace the MQAM modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the MQAM modulator.
- 2 Contact Cisco Services for further assistance.

MQAM Modulator Alarm ID 57 (39 Hex)

The **ASI2 MPEG Packets Error** alarm occurs when there are errors in the headers of the MPEG packets at the DVB ASI Input 2 port in the MQAM modulator. Errors include an invalid MPEG packet header where the first byte (for example, sync byte) is not equal to 47 Hex (0x47), or where the MPEG packet size is not exactly 188 bytes. There is potential loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the MQAM modulator that is sending this alarm.

This alarm may also occur when the DVB ASI cable is disconnected and then clear before you reconnect the cable. This clear occurs because the MPEG stream is disrupted and the device detects that the input signal is completely lost.

Note: This alarm is self-clearing and may be intermittent. Single instances of this alarm that clear automatically and that do not reappear are not a cause for concern.

Front Panel Message

ASI2 Errored MPEG packet

Possible Cause(s)

- A cable is loose, disconnected, or defective.
- There are data errors on the satellite link.
- The rate of change of the IEC exceeds the allowed threshold.
- Upstream devices that provide input to the MQAM modulator are sending errored MPEG packets.
- There is defective local MPEG coding.
- The MQAM modulator is defective.

Check and Correct

A cable is loose, disconnected, or defective

Check for loose connections or defective cables, tighten any loose cable connections, connect any disconnected cables, and replace any defective cables.

Note: This alarm may also occur when the DVB ASI cable is disconnected and then clear before you reconnect the cable. This is normal.

Data errors on the satellite link

Contact your signal provider to verify if there are any problems with their satellite transmissions.

IEC exceeds threshold

Clean up the MPEG signal input to the MQAM modulator by checking the IRT, RTE, and MPEG encoder.

Upstream devices sending errored MPEG packets

- 1 Check the upstream devices that are sending MPEG packets to the DVB ASI input ports on the MQAM modulator.
- 2 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 3 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 4 If the alarm continues to occur, contact Cisco Services for further assistance.

Defective local MPEG coding

Check the local source devices that are providing MPEG content to the MQAM modulator.

MQAM modulator is defective

- 1 Replace the MQAM modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the MQAM modulator.
- 2 Contact Cisco Services for further assistance.

MQAM Modulator Alarm ID 58 (3A Hex)

The **ASI2 FIFO Overflow Error** alarm occurs when there is a FIFO buffer overflow at the DVB ASI Input 2 port on the MQAM modulator, and packet data is lost. There is a potential for loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the MQAM modulator that is sending this alarm.

Front Panel Message

ASI2 FIFO overflow

Possible Cause(s)

- The data rate as defined from the EC for the MQAM modulator sessions is too low, which also means that the data rate of the ASI input to the MQAM modulator is too high.
- There are too many sessions defined for the MQAM modulator from the EC.
- The modulation mode is incorrect.
- Upstream devices are sending too many MPEG packets to the MQAM modulator.
- A hardware problem occurred.

Check and Correct

Data rate is too low

- 1 Reduce the amount of incoming data.
- 2 Reduce the amount of data added to the stream.
- 3 Increase the MQAM modulation mode.
- 4 Verify and correct session rate targets and threshold values.

Too many sessions defined

Reduce the total number of MPEG programs by deleting sessions.

Modulation mode is incorrect

Verify and correct the modulation mode.

Upstream devices sending too many MPEG packets

Check the upstream devices that are sending MPEG packets to the DVB ASI input ports on the MQAM modulator.

Hardware problem

- 1** Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 2** Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 3** Replace the MQAM modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the MQAM modulator.
- 4** If the alarm continues to occur, contact Cisco Services for further assistance.

MQAM Modulator Alarm ID 59 (3B Hex)

The **ASI2 Excess Packets Dumped** alarm occurs when there is excessive bandwidth utilization on one or more channels at the DVB ASI Input 2 port on the MQAM modulator. Packets for those channels are being dumped so as not to affect the other channels.

There is potential loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the MQAM modulator that is sending this alarm.

Note: This alarm is self-clearing and may be intermittent. Single instances of this alarm that clear automatically and that do not reappear are not a cause for concern.

Front Panel Message

ASI2 Packets were dumped

Possible Cause(s)

- The data rate as defined from the EC for the MQAM modulator sessions is too low, which also means that the data rate of the ASI input to the MQAM modulator is too high.
- There are too many sessions defined for the MQAM modulator from the EC.
- The modulation mode is incorrect.
- Upstream devices are sending too many MPEG packets to the MQAM modulator.
- A hardware problem occurred.

Check and Correct

Data rate is too low

- 1 Reduce the amount of incoming data.
- 2 Reduce the amount of data added to the stream.
- 3 Increase the MQAM modulation mode.
- 4 Verify and correct session rate targets and threshold values.

Too many sessions defined

Reduce the total number of MPEG programs by deleting sessions.

Modulation mode is incorrect

Verify and correct the modulation mode.

Upstream devices sending too many MPEG packets

Check the upstream devices that are sending MPEG packets to the DVB ASI input ports in the MQAM modulator.

Hardware problem

- 1 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 2 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 3 Replace the MQAM modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the MQAM modulator.
- 4 If the alarm continues to occur, contact Cisco Services for further assistance.

MQAM Modulator Alarm ID 60 (3C Hex)

The **RF OUT 1 Low Priority Packets Dropped** alarm occurs when the MQAM modulator is dropping low priority packets at RF OUT 1. Low priority packets are being dropped because the number of packets at RF OUT 1 exceeds its capacity.

Note: This alarm is self-clearing and may be intermittent. Single instances of this alarm that clear automatically and that do not reappear are not a cause for concern.

There is a low potential for loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the MQAM modulator that is sending this alarm.

Front Panel Message

OUT1 Packets dropped

Possible Cause(s)

- The data rate as defined from the EC for the MQAM modulator sessions is too low, which also means that the data rate of the ASI input to the MQAM modulator is too high.
- There are too many sessions defined for the MQAM modulator from the EC.
- The modulation mode is incorrect.
- A hardware problem occurred.

Check and Correct

Data rate is too low

- 1 Reduce the amount of incoming data.
- 2 Reduce the amount of data added to the stream.
- 3 Increase the MQAM modulation mode.
- 4 Verify and correct session rate targets and threshold values.

Too many sessions defined

Reduce the total number of MPEG programs by deleting sessions.

Modulation mode is incorrect

Verify and correct the modulation mode.

Hardware problem

- 1** Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 2** Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 3** Replace the MQAM modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the MQAM modulator.
- 4** If the alarm continues to occur, contact Cisco Services for further assistance.

MQAM Modulator Alarm ID 61 (3D Hex)

The **RF OUT 2 Low Priority Packets Dropped** alarm occurs when the MQAM modulator is dropping low priority packets at RF OUT 2. Low priority packets are being dropped because the number of packets at RF OUT 2 exceeds its capacity.

Note: This alarm is self-clearing and may be intermittent. Single instances of this alarm that clear automatically and that do not reappear are not a cause for concern.

There is a low potential for loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the MQAM modulator that is sending this alarm.

Front Panel Message

OUT2 Packets dropped

Possible Cause(s)

- The data rate as defined from the EC for the MQAM modulator sessions is too low, which also means that the data rate of the ASI input to the MQAM modulator is too high.
- There are too many sessions defined for the MQAM modulator from the EC.
- The modulation mode is incorrect.
- A hardware problem occurred.

Check and Correct

Data rate is too low

- 1 Reduce the amount of incoming data.
- 2 Reduce the amount of data added to the stream.
- 3 Increase the MQAM modulation mode.
- 4 Verify and correct session rate targets and threshold values.

Too many sessions defined

Reduce the total number of MPEG programs by deleting sessions.

Modulation mode is incorrect

Verify and correct the modulation mode.

Hardware problem

- 1** Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 2** Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 3** Replace the MQAM modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the MQAM modulator.
- 4** If the alarm continues to occur, contact Cisco Services for further assistance.

MQAM Modulator Alarm ID 62 (3E Hex)

The **RF OUT 3 Low Priority Packets Dropped** alarm occurs when the MQAM modulator is dropping low priority packets at RF OUT 3. Low priority packets are being dropped because the number of packets at RF OUT 3 exceeds its capacity.

Note: This alarm is self-clearing and may be intermittent. Single instances of this alarm that clear automatically and that do not reappear are not a cause for concern.

There is a low potential for loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the MQAM modulator that is sending this alarm.

Front Panel Message

OUT3 Packets dropped

Possible Cause(s)

- The data rate as defined from the EC for the MQAM modulator sessions is too low, which also means that the data rate of the ASI input to the MQAM modulator is too high.
- There are too many sessions are defined for the MQAM modulator from the EC.
- The modulation mode is incorrect.
- A hardware problem occurred.

Check and Correct

Data rate is too low

- 1 Reduce the amount of incoming data.
- 2 Reduce the amount of data added to the stream.
- 3 Increase the MQAM modulation mode.
- 4 Verify and correct session rate targets and threshold values.

Too many sessions defined

Reduce the total number of MPEG programs by deleting sessions.

Modulation mode is incorrect

Verify and correct the modulation mode.

Hardware problem

- 1** Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 2** Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 3** Replace the MQAM modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the MQAM modulator.
- 4** If the alarm continues to occur, contact Cisco Services for further assistance.

MQAM Modulator Alarm ID 63 (3F Hex)

The **RF OUT 4 Low Priority Packets Dropped** alarm occurs when the MQAM modulator is dropping low priority packets at RF OUT 4. Low priority packets are being dropped because the number of packets at RF OUT 4 exceeds its capacity.

Note: This alarm is self-clearing and may be intermittent. Single instances of this alarm that clear automatically and that do not reappear are not a cause for concern.

There is a low potential for loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the MQAM modulator that is sending this alarm.

Front Panel Message

OUT4 Packets dropped

Possible Cause(s)

- The data rate as defined from the EC for the MQAM modulator sessions is too low, which also means that the data rate of the ASI input to the MQAM modulator is too high.
- There are too many sessions defined for the MQAM modulator from the EC.
- The modulation mode is incorrect.
- A hardware problem occurred.

Check and Correct

Data rate is too low

- 1 Reduce the amount of incoming data.
- 2 Reduce the amount of data added to the stream.
- 3 Increase the MQAM modulation mode.
- 4 Verify and correct session rate targets and threshold values.

Too many sessions defined

Reduce the total number of MPEG programs by deleting sessions.

Modulation mode is incorrect

Verify and correct the modulation mode.

Hardware problem

- 1** Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 2** Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 3** Replace the MQAM modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the MQAM modulator.
- 4** If the alarm continues to occur, contact Cisco Services for further assistance.

MQAM Modulator Alarm ID 64 (40 Hex)

The **Hardware Failure** alarm occurs when there is a hardware failure in the MQAM modulator. When this condition exists, there is a potential for loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the MQAM modulator that is sending this alarm.

Front Panel Message

Hardware error

Possible Cause(s)

A hardware failure occurred.

Check and Correct

- 1 Power down and then power up the MQAM modulator using the on/off rocker-type switch on the back panel, or reset the MQAM modulator from the EC.
- 2 Replace the MQAM modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the MQAM modulator.
- 3 If the alarm continues to occur, contact Cisco Services for further assistance.

MQAM Modulator Alarm ID 65 (41 Hex)

The **Software Runtime Error** alarm displays when low-level software errors occur in the MQAM modulator. When this condition exists, there is a potential for loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the MQAM modulator that is sending this alarm.

Front Panel Message

Runtime error

Possible Cause(s)

Low-level software errors occurred.

Check and Correct

- 1 If this alarm continues to occur, power down and then power up the MQAM modulator using the on/off rocker-type switch on the back panel, or reset the MQAM modulator from the EC.
- 2 If resetting the MQAM modulator does not solve the problem, contact Cisco Services for further assistance.

MQAM Modulator Alarm ID 66 (42 Hex)

The **Craft Port Activity** status event occurs when a user or a system operator uses the craft port to view or change the settings on the MQAM modulator. There is a potential for loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the MQAM modulator that is sending this event.

Front Panel Message

Craft event change

Possible Cause(s)

A user or a system operator viewed or changed the settings on the MQAM modulator from the craft port.

Check and Correct

- 1 Check to see if any settings were changed.
- 2 Are all services functioning correctly?
 - If **yes**, no further action is required.
 - If **no**, go to step 3.
- 3 Restore the settings to the previous configuration.
- 4 Power down and then power up the MQAM modulator using the on/off rocker-type switch on the back panel, or reset the MQAM modulator from the EC to restore the previous configuration.
- 5 If resetting the MQAM modulator does not solve the problem, contact Cisco Services for further assistance.

MQAM Modulator Alarm ID 67 (43 Hex)

The **Front Panel Changed** status event occurs when a user or a system operator uses the front panel keys to change the settings on the MQAM modulator. There is a potential for loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the MQAM modulator that is sending this event.

Front Panel Message

Front panel event change

Possible Cause(s)

A user or a system operator changed the settings on the MQAM modulator using the front panel keys.

Check and Correct

- 1 Verify what settings were changed.
- 2 Are all services functioning correctly?
 - If **yes**, no further action is required.
 - If **no**, go to step 3.
- 3 Restore the settings to the previous configuration.
- 4 Power down and then power up the MQAM modulator using the on/off rocker-type switch on the back panel, or reset the MQAM modulator from the EC to restore the previous configuration.
- 5 If resetting the MQAM modulator does not solve the problem, contact Cisco™ Broadband Services for further assistance.

MQAM Modulator Alarm ID 68 (44 Hex)

The **RF OUT 1 FIFO Overflow** alarm occurs when there is a FIFO overflow at RF OUT 1 on the MQAM modulator, and packet data is lost. There is a low potential for loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the MQAM modulator that is sending this alarm.

Note: This alarm is self-clearing and may be intermittent. Single instances of this alarm that clear automatically and that do not reappear are not a cause for concern.

Front Panel Message

OUT1 FIFO Overflow

Possible Cause(s)

- The data rate as defined from the EC for the MQAM modulator sessions is too low, which also means that the data rate of the ASI input to the MQAM modulator is too high.
- There are too many sessions defined for the MQAM modulator from the EC.
- The modulation mode is incorrect.
- A hardware problem occurred.

Check and Correct

Data rate is too low

- 1 Reduce the amount of incoming data.
- 2 Reduce the amount of data added to the stream.
- 3 Increase the MQAM modulation mode.
- 4 Verify and correct session rate targets and threshold values.

Too many sessions defined

Reduce the total number of MPEG programs by deleting sessions.

Modulation mode is incorrect

Verify and correct the modulation mode.

Hardware problem

- 1 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 2 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 3 If the alarm continues to occur, contact Cisco Services for further assistance.

MQAM Modulator Alarm ID 69 (45 Hex)

The **RF OUT 2 FIFO Overflow** alarm occurs when there is a FIFO overflow at RF OUT 2 on the MQAM modulator, and packet data is lost. There is a low potential for loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the MQAM modulator that is sending this alarm.

Note: This alarm is self-clearing and may be intermittent. Single instances of this alarm that clear automatically and that do not reappear are not a cause for concern.

Front Panel Message

OUT2 FIFO Overflow

Possible Cause(s)

- The data rate as defined from the EC for the MQAM modulator sessions is too low, which also means that the data rate of the ASI input to the MQAM modulator is too high.
- There are too many sessions defined for the MQAM modulator from the EC.
- The modulation mode is incorrect.
- A hardware problem occurred.

Check and Correct

Data rate is too low

- 1 Reduce the amount of incoming data.
- 2 Reduce the amount of data added to the stream.
- 3 Increase the MQAM modulation mode.
- 4 Verify and correct session rate targets and threshold values.

Too many sessions defined

Reduce the total number of MPEG programs by deleting sessions.

Modulation mode is incorrect

Verify and correct the modulation mode.

Hardware problem

- 1 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 2 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 3 If the alarm continues to occur, contact Cisco Services for further assistance.

MQAM Modulator Alarm ID 70 (46 Hex)

The **RF OUT 3 FIFO Overflow** alarm occurs when there is a FIFO overflow at RF OUT 3 on the MQAM modulator, and packet data is lost. There is a low potential for loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the MQAM modulator that is sending this alarm.

Note: This alarm is self-clearing and may be intermittent. Single instances of this alarm that clear automatically and that do not reappear are not a cause for concern.

Front Panel Message

OUT3 FIFO Overflow

Possible Cause(s)

- The data rate as defined from the EC for the MQAM modulator sessions is too low, which also means that the data rate of the ASI input to the MQAM modulator is too high.
- There are too many sessions defined for the MQAM modulator from the EC.
- The modulation mode is incorrect.
- A hardware problem occurred.

Check and Correct

Data rate is too low

- 1 Reduce the amount of incoming data.
- 2 Reduce the amount of data added to the stream.
- 3 Increase the MQAM modulation mode.
- 4 Verify and correct session rate targets and threshold values.

Too many sessions defined

Reduce the total number of MPEG programs by deleting sessions.

Modulation mode is incorrect

Verify and correct the modulation mode.

Hardware problem

- 1 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 2 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 3 If the alarm continues to occur, contact Cisco Services for further assistance.

MQAM Modulator Alarm ID 71 (47 Hex)

The **RF OUT 4 FIFO Overflow** alarm occurs when there is a FIFO overflow at RF OUT 4 on the MQAM modulator, and packet data is lost. There is a low potential for loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the MQAM modulator that is sending this alarm.

Note: This alarm is self-clearing and may be intermittent. Single instances of this alarm that clear automatically and that do not reappear are not a cause for concern.

Front Panel Message

OUT4 FIFO Overflow

Possible Cause(s)

- The data rate as defined from the EC for the MQAM modulator sessions is too low, which also means that the data rate of the ASI input to the MQAM modulator is too high.
- There are too many sessions defined for the MQAM modulator from the EC.
- The modulation mode is incorrect.
- A hardware problem occurred.

Check and Correct

Data rate is too low

- 1 Reduce the amount of incoming data.
- 2 Reduce the amount of data added to the stream.
- 3 Increase the MQAM modulation mode.
- 4 Verify and correct session rate targets and threshold values.

Too many sessions defined

Reduce the total number of MPEG programs by deleting sessions.

Modulation mode is incorrect

Verify and correct the modulation mode.

Hardware problem

- 1 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 2 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 3 If the alarm continues to occur, contact Cisco Services for further assistance.

MQAM Modulator Alarm ID 72 (48 Hex)

The **3rd Party CA Not Provisioned** alarm occurs when an SCS MQAM modulator does not receive the *qprovisionThirdPartyCaResponse* CA message from the EC. The MQAM modulator will not attempt to connect to external devices such as the EIS and the ECMG while this alarm is active. There is a potential for loss of programming content relative to the MQAM modulator that is sending this alarm.

Important! This alarm occurs only on MQAM modulators configured as SCS MQAM modulators.

Front Panel Message

3rd party ca not provisioned

Possible Cause(s)

SCS MQAM failed to connect to the EC qamManager process.

Check and Correct

- 1 Check for loose connections or defective cables, tighten any loose cable connections, connect any disconnected cables, and replace any defective cables.
- 2 Verify that the qamManager process on the EC is running.
- 3 If the alarm continues to occur, contact Cisco Services for further assistance.

MQAM Modulator Alarm ID 73 (49 Hex)

The **Primary EIS Not Connected** alarm is sent one time when the TCP/IP link is established, but an SCS MQAM modulator is not communicating with the Primary EIS. This alarm remains active until the Primary EIS establishes communication at which time the SCS MQAM modulator clears the alarm. There is a potential for loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the MQAM modulator that is sending this alarm. This alarm also indicates that the signal is being transmitted in the clear, when it should be encrypted.

Note: This alarm will only be sent again one time if the Primary EIS establishes communication and subsequently fails.

Important! This alarm occurs only on MQAM modulators configured as SCS MQAM modulators.

Front Panel Message

no connect primary eis

Possible Cause(s)

- Cables are loose, disconnected, or defective.
- The EIS connection parameters in the EC are not correct.

Check and Correct

- 1 Check for loose connections or defective cables, tighten any loose cable connections, connect any disconnected cables, and replace any defective cables.
- 2 Check and verify the EIS connection parameters in the EC.
- 3 If the alarm continues to occur, contact Cisco Services for further assistance.

MQAM Modulator Alarm ID 74 (4A Hex)

The **Secondary EIS Not Connected** alarm occurs when an SCS MQAM modulator loses the primary connection to the EIS and is unable to establish the secondary EIS connection. There is a potential for loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the MQAM modulator that is sending this alarm. This alarm also indicates that the signal is being transmitted in the clear, when it should be encrypted.

Important! This alarm occurs only on MQAM modulators configured as SCS MQAM modulators.

Front Panel Message

no connect secondary eis

Possible Cause(s)

Cables are loose, disconnected, or defective.

The EIS connection parameters in the EC are not correct.

Check and Correct

- 1 Check for loose connections or defective cables, tighten any loose cable connections, connect any disconnected cables, and replace any defective cables.
- 2 Check and verify the EIS connection parameters in the EC.
- 3 If the alarm continues to occur, contact Cisco Services for further assistance.

MQAM Modulator Alarm ID 75 (4B Hex)

The **Primary ECMG Not Connected** alarm is sent one time when the TCP/IP link is established, but an SCS MQAM modulator is unable to communicate with the Primary ECMG. This alarm remains active until the Primary ECMG establishes communication at which time it is deactivated. This alarm will only be sent again one time if the Primary ECMG establishes communication and subsequently fails. Connection to the Secondary ECMG is an available option.

There is a potential for loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the MQAM modulator that is sending this alarm. This alarm also indicates that the signal is being transmitted in the clear, when it should be encrypted.

Note: The SCS MQAM modulator will alternately seek to establish a TCP/IP link and a communication links with the Primary and Secondary ECMGs until one of the communication links succeeds. When a communication link is established, if any ECMG link/connection alarms are active, the SCS MQAM modulator clears those alarms.

Important! This alarm occurs only on MQAM modulators configured as SCS MQAM modulators.

Front Panel Message

no connect primary ECMG

Possible Cause(s)

- Cables are loose, disconnected, or defective.
- The primary ECMG connection parameters are incorrect.

Check and Correct

- 1 Check for loose connections or defective cables, tighten any loose cable connections, connect any disconnected cables, and replace any defective cables.
- 2 Check and verify the CAS ID parameters in the EC.
- 3 If the alarm continues to occur, contact Cisco Services for further assistance.

MQAM Modulator Alarm ID 76 (4C Hex)

The **Secondary ECMG Not Connected** alarm is sent one time when the TCP/IP link is established, but an SCS MQAM modulator is unable to communicate with the Secondary ECMG. This alarm remains active until the Secondary ECMG establishes communication at which time the SCS MQAM modulator clears the alarm. This alarm will only be sent again one time if the Secondary ECMG establishes communication and then subsequently fails.

There is a potential for loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the MQAM modulator that is sending this alarm. This alarm also indicates that the signal is being transmitted in the clear, when it should be encrypted.

Note: The SCS MQAM modulator will alternately seek to establish TCP/IP link and communication links with the Primary and Secondary ECMGs until one of the communications links succeeds. When a communication link is established, if any ECMG link/connection alarms are active, the SCS MQAM modulator clears those alarms.

Important: This alarm occurs only on MQAM modulators configured as SCS MQAM modulators.

Front Panel Message

no connect secondary ECMG

Possible Cause(s)

- Cables are loose, disconnected, or defective.
- The secondary ECMG connection parameters are incorrect.

Check and Correct

- 1 Check for loose connections or defective cables, tighten any loose cable connections, connect any disconnected cables, and replace any defective cables.
- 2 Check and verify the CAS ID parameters in the EC.
- 3 If the alarm continues to occur, contact Cisco Services for further assistance.

MQAM Modulator Alarm ID 77 (4D Hex)

The **EIS Link Lost** alarm is sent one time by the SCS MQAM modulator when the TCP/IP link has not been established with the Primary EIS. This alarm will only be sent again one time if the TCP/IP link is established with the Primary EIS and then subsequently fails.

There is a potential for loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the MQAM modulator that is sending this alarm. This alarm also indicates that the signal is being transmitted in the clear, when it should be encrypted.

Note: The SCS MQAM modulator will continually attempt to establish a TCP/IP link and communication with the Primary EIS until a TCP/IP link and communication is established. When a communication link is established, if any EIS link/connection alarms are active, the SCS MQAM modulator clears those alarms.

Important: This alarm occurs only on MQAM modulators configured as SCS MQAM modulators.

Front Panel Message

EIS link lost

Possible Cause(s)

- Cables are loose, disconnected, or defective.
- The EIS is not operational.

Check and Correct

- 1 Check for loose connections or defective cables, tighten any loose cable connections, connect any disconnected cables, and replace any defective cables.
- 2 Verify that the EIS is operating correctly.
- 3 If the alarm continues to occur, contact Cisco Services for further assistance.

MQAM Modulator Alarm ID 78 (4E Hex)

The **ECMG Link Lost** alarm is sent when an SCS MQAM modulator has not established a TCP/IP link with the Primary ECMG. This alarm will only be sent again one time if the TCP/IP link is established with the Primary ECMG and then subsequently fails.

There is a potential for loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the MQAM modulator that is sending this alarm. This alarm also indicates that the signal is being transmitted in the clear, when it should be encrypted.

Note: The SCS MQAM modulator will alternately seek to establish a TCP/IP link and a communication links with the Primary and Secondary ECMGs until one of the communication links succeeds. When a communication link is established, if any ECMG link/connection alarms are active, the SCS MQAM modulator clears those alarms.

Important: This alarm occurs only on MQAM modulators configured as SCS MQAM modulators.

Front Panel Message

ECMG link lost

Possible Cause(s)

- Cables are loose, disconnected, or defective.
- The ECMG is not operational.

Check and Correct

- 1 Check for loose connections or defective cables, tighten any loose cable connections, connect any disconnected cables, and replace any defective cables.
- 2 Check and verify that the ECMG is operating correctly.
- 3 If the alarm continues to occur, contact Cisco Services for further assistance.

MQAM Modulator Alarm ID 79 (4F Hex)

The **SCG Received for Non-Existent Session** alarm occurs when an SCS MQAM modulator receives SCG information for a session that does not exist on the SCS MQAM modulator. The SCS MQAM modulator clears this alarm immediately.

Important: This alarm occurs only on MQAM modulators configured as SCS MQAM modulators.

Front Panel Message

no mqam session

Possible Cause(s)

The parameters in the SCG message do not match any existing sessions provisioned on the SCS MQAM modulator.

Check and Correct

- 1 Check the SCS scheduler.
- 2 If the alarm continues to occur, contact Cisco Services for further assistance.

MQAM Modulator Alarm ID 128 (80 Hex) through Alarm ID 1151 (47F Hex)

The **Session Data Error** alarm occurs when the MQAM modulator detects a session data error and indicates one of the following conditions:

- Underflow and overflow errors indicate that the data flow for the session is more or less than what has been defined by the EC for the session.

Important: The default threshold for the underflow and overflow alarms is zero. Note that the same threshold parameter is utilized for determining both underflow and overflow. The algorithm for determining underflow/overflow is as follows:

- When the threshold value is not provisioned by a management entity, the threshold value is 0 and the UNDERFLOW alarm will occur if the session's data rate falls below 1 bit per second (bps) (i.e., either equal to 0 bps or a fractional value that is less than 1 bps). In other words, the Overflow alarm is essentially disabled.
- When a management entity provisions the alarm with a non-zero threshold value, the UNDERFLOW alarm occurs when the measured session data rate falls below (sessionRate - threshold) and the OVERFLOW alarm occurs when the measured session data rate exceeds (sessionRate + threshold).
- PID enable errors indicate that a PID for this session is not enabled in the MQAM modulator.

Note: sessionRate is the rate that was specified createSession request.

Session data alarm IDs 128 (decimal) through 1151 (decimal) represent Session Data alarms. Sessions correspond to MPEG programs. There can be up to 256 simultaneous sessions on each MQAM modulator RF output port. Because there are four RF output ports in each MQAM modulator, this means that there can be up to 1,024 simultaneous sessions per MQAM modulator. Each of these sessions will generate a unique Alarm ID when a Session Data Error occurs for that session. The internal sessions indices 0 through 1023 on the MQAM modulator are mapped to session data error Alarm IDs 128 (decimal) through 1151 (decimal).

Note: If the session rate is 0 (zero) bps, an error will always be detected regardless of the session rate and threshold values. A session rate of zero results from a loss of input signal. Therefore, all provisioned sessions will report session data alarms if there is a loss of input signal.

MQAM Modulator Alarm ID 128 (80 Hex) through Alarm ID 1151 (47F Hex)

There is potential loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the MQAM modulator that is sending this alarm.

Important: The **Additional Information** field in the Alarm Manager window displays the Session ID number, the Input port number, the Output port number, and the Cause Code.

Front Panel Message

Session xxxx data error

Note: Session front panel messages display a number representing the internal session number used by the MQAM modulator. The number is between 0000 and 1023, and is shown as a decimal value.

Possible Cause(s)

The data flow for the session is more or less than what is defined by the EC for the session, or a PID that should be enabled in the MQAM modulator hardware is not enabled. This indicates one or more of the following conditions:

- Loss of input signal
- Cause Code 1 - Underflow conditions - The session data rate for this session drops to 0 (zero) or is less than expected.
Important: The session rate dropping to 0 (zero) triggers an underflow alarm, but is not the result of a loss of signal condition. When a loss of signal occurs, the underflow alarm is not reported. This prevents the system from being overwhelmed with a large number of session data alarms. Alarms that occur as a result of higher level alarms are not reported.
- Cause Code 2 - Overflow conditions - The data rate for this session exceeds the provisioned data rate.
- Cause Code 3 - PID enable error - A PID associated that should be enabled is not enabled in the MQAM modulator.
- Cause Code 4 - Data drop scheduled
- Cause Code 5 - Data overflow and drop scheduled

Check and Correct

Loss of input signal

Check for loose cable connections or defective cables, then tighten any loose cable connections, and replace any defective cables.

Chapter 2 MQAM Modulator Alarms

Overflow and underflow conditions

- 1 Verify and correct any session setup problems, including the session rate target and threshold values.
- 2 If loss of input signal is the cause, restore the input signal.
- 3 For the *overflow* condition, teardown, rebuild, and then restart the session using a higher bandwidth.
- 4 If the session setup data is correct, the data is becoming corrupted.
- 5 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 6 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report. If you cannot resolve these issues, contact Cisco Services.

PID issues

- 1 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 2 Tear down and restart the session. If the alarm reoccurs the PID is missing from the input stream.
- 3 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report. If you cannot resolve these issues, contact Cisco Services.

MQAM Modulator Alarm ID 1152 (480 Hex) through Alarm ID 2175 (87F Hex)

The **Session Program Error** alarm occurs when there are errors or other problems in the input source for the session.

Alarm IDs 1152 (decimal) through 2175 (decimal) represent Session Program Error alarms. Sessions correspond to MPEG programs. There can be up to 256 simultaneous sessions on each MQAM modulator RF output port. Because there are four RF output ports in each MQAM modulator, this means that there can be up to 1,024 simultaneous sessions on each MQAM modulator. Each of these sessions will generate a unique Alarm ID when a Session Program Error occurs for that session. The internal sessions indices 0 through 1023 on the MQAM modulator are mapped to session program Alarm IDs 1152 (decimal) through 2175 (decimal).

There is a potential for loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the MQAM modulator that is sending this alarm.

Important: The **Additional Information** field in the Alarm Manager window displays the Session ID number, the Input port number, the Output port number, and the Cause Code.

Front Panel Message

Session xxxx prog error

Note: Session front panel messages display a number representing the internal session number used by the MQAM modulator. The number is between 0000 and 1023, and is shown as a decimal value.

Possible Cause(s)

- Cause Code 1 - A CRC error was detected on a PMT.
- Cause Code 2 - A new PMT was detected.
- Cause Code 3 - An attempt to create a session failed. This cause code displays when the PIDs in the PMT do not agree with those specified in the session setup message, and they do not conflict with any existing session's PIDs. (This cause code occurs only on SCS MQAMs)
- Cause Code 4 - Create session failed with PID conflict. This cause code displays when the PIDs in the PMT do not agree with those specified in the session setup message, but they do conflict with an existing session's PIDs. (**This cause code occurs only on SCS MQAMs**)

Chapter 2 MQAM Modulator Alarms

- Cause Code 5 - PMT update. This cause code displays when a PMT update is received and the PIDs do not agree with those specified in the session setup message, and they do not conflict with any existing session's PIDs. **(This cause code occurs only on SCS MQAMs)**
- Cause Code 6 - PMT update. This cause code displays when a PMT update is received, and the PIDs do not agree with those specified in the session message, but they do conflict with an existing session's PIDs. **(This cause code occurs only on SCS MQAMs)**
- The PSI table data for the session contains errors.

Check and Correct

CRC error detected

Delete the session

New PMT detected

This is for information only. No action is required.

Create a session failed

Teardown and rebuild the session using PID values that do not create conflicts.

Create session failed with PID conflict

Teardown and rebuild the session using PID values that do not create conflicts.

PMT update, no conflict

Teardown and rebuild the session using PID values that do not create conflicts.

PMT update with conflict

Teardown and rebuild the session using PID values that do not create conflicts.

PSI table contains errors

Check the upstream MPEG input sources connected to the MQAM modulator.

MQAM Modulator Alarm ID 2176 (880 Hex) through Alarm ID 3199 (C7F Hex)

The **Session Conditional Access Error** alarm occurs when the MQAM modulator detects an error in the CA encryption for a session. This alarm indicates that the signal is being transmitted in the clear, when it should be encrypted.

Alarm IDs 2176 (decimal) through 3199 (decimal) represent Session Conditional Access alarms. Sessions correspond to MPEG programs. There can be up to 256 simultaneous sessions on each MQAM modulator RF output port. Because there are four RF output ports in each MQAM modulator, this means that there can be up to 1,024 simultaneous sessions on each MQAM modulator. Each of these sessions will generate a unique Alarm ID when a Session Conditional Access Error occurs. Session CA alarms for internal session indices 0 through 1023 on the MQAM modulator are mapped to the session CA alarm IDs 2176 through 3199.

Important: When this condition exists, certain sessions may be broadcast without encryption, impacting potential pay-per-view and subscription revenues, and resulting in some subscribers receiving channels and services they do not want.

There is a potential for loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the MQAM modulator that is sending this alarm.

Important: The **Additional Information** field in the Alarm Manager window displays the Session ID number, the Input port number, and the Output port number.

Front Panel Message

Session xxxx ca error

Note: Session front panel messages display a number representing the internal session number used by the MQAM modulator. The number is between 0000 and 1023, and is shown as a decimal value.

Possible Cause(s)

- CA failed.
- The CA settings are improper.
- A bad ISK VOD session.
- Hardware failure.

Check and Correct

CA failed

Delete the failed session.

Chapter 2 MQAM Modulator Alarms

CA settings improper

Check and correct the CA settings on the EC.

Bad ISK message

- 1 Troubleshoot CA on the EC.
- 2 Contact Cisco Services.

Hardware failure

- 1 Replace the MQAM modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the MQAM modulator.
- 2 Contact Cisco Services for further assistance.

3

GQAM Modulator Alarms

Introduction

This chapter provides detailed information for troubleshooting the alarms that are generated by the GQAM modulator. The alarms are arranged in the ascending numeric order of the Alarm IDs. For your convenience, the Alarm IDs are listed in both decimal and hexadecimal format. You can look up the possible causes and then follow the check and correct procedures for each alarm to help you troubleshoot and clear each alarm.

GQAM Modulator Alarm ID 1 (1 Hex)

The **RF1 Communication Error** alarm occurs when the digital I/O board in the GQAM modulator cannot communicate with the RF MCU at RF OUT 1. When this alarm occurs, video is not transmitted through the RF OUT 1 port.

Front Panel Message

RF1 Comm. failure

Possible Cause(s)

- The digital I/O board cannot communicate with the MCU on the GQAM modulator RF board at RF OUT 1.
- The MCU at RF OUT 1 on the GQAM modulator is not programmed correctly.
- The CRC checksum error did not clear correctly.
- The power supply failed or is failing.

Check and Correct

Digital I/O board cannot communicate with the MCU

Check for loose connections or defective cables, tighten any loose cables, and replace any defective cables.

MCU not programmed correctly

- 1 Power down and then power up the GQAM modulator using the on/off rocker-type switch on the back panel, or reset the GQAM modulator from the EC.
- 2 If resetting the GQAM modulator does not correct the problem, contact Cisco Services.

CRC checksum error

CRC errors are transient and intermittent and clear automatically.

Power supply failure

Replace the GQAM modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the GQAM modulator.

GQAM Modulator Alarm ID 2 (2 Hex)

The **RF1 Excessive Temperature** alarm occurs when the internal temperature of the GQAM modulator exceeds 70°C (158°F). A GQAM modulator that is overheating could have minimal to severe impact on services. If the modulator fails due to overheating, there would be no services available from that GQAM modulator.

Front Panel Message

RF1 Exceeded max temp

Possible Cause(s)

- The vents on the GQAM modulator are blocked.
- The room temperature is too high.
- A fan failure occurred.
- A hardware failure occurred.

Check and Correct

Vents are blocked

Check and clear any obstructions from the vents.

Room temperature is too high

Check and repair or replace the heating/cooling equipment in the room.

Fan failure

Check and repair or replace the fan.

Hardware failure

- 1 Replace the GQAM modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the GQAM modulator.
- 2 If the alarm condition continues to occur, contact Cisco Services.

GQAM Modulator Alarm ID 3 (3 Hex)

The **RF1 Power Supply Failure** alarm occurs when at least one internal power supply in the GQAM modulator fails. There is no RF output at RF OUT 1 when this condition exists, and video is not transmitted through the RF OUT 1 port. This condition could also generate a communication alarm. No services are available through the RF OUT 1 port.

Front Panel Message

RF1 Power supply failure

Possible Cause(s)

The internal power supply to RF OUT 1 in the GQAM modulator has failed or is failing.

Note: The RF output field on the front panel LCD screen displays “MUTED” when this condition exists.

Check and Correct

- 1 Check power source, power wires, and the on/off rocker-type switch on the back panel of the GQAM modulator.
- 2 Replace the GQAM modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the GQAM modulator.
- 3 Contact Cisco Services for further assistance.

GQAM Modulator Alarm ID 4 (4 Hex)

The **RF1 DC Lock Detect Error** alarm occurs when the DC lock detect signal at RF OUT 1 in the GQAM modulator is functioning incorrectly. There is no RF output at RF OUT 1 when this condition exists, and video is not transmitted through the RF OUT 1 port.

Front Panel Message

RF1 DC Lock detect error

Possible Cause(s)

- The DC lock detect signal at RF OUT 1 in the GQAM modulator is functioning incorrectly.
- During the MCU POST, the lock detect signal from the DC PLL at RF OUT 1 in the GQAM modulator did not indicate an unlocked condition when one existed.
- The output converter synthesizer in the GQAM modulator has malfunctioned.
Note: The RF output field on the front panel LCD screen displays “MUTED” when this condition exists.

Check and Correct

- 1 Power down and then power up the GQAM modulator using the on/off rocker-type switch on the back panel, or reset the GQAM modulator from the EC.
- 2 Replace the GQAM modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing and repairing the GQAM modulator.
- 3 Contact Cisco Services for further assistance.

GQAM Modulator Alarm ID 5 (5 Hex)

The **RF1 DC PLL Unlocked Error** alarm occurs when the DC PLL synthesizer at RF OUT 1 in the GQAM modulator cannot lock. There is no RF output at RF OUT 1 when this condition exists because the signal is not synchronized, and video is not transmitted through the RF OUT 1 port.

Front Panel Message

RF1 DC PLL unlocked

Possible Cause(s)

- The DC PLL synthesizer at RF OUT 1 in the GQAM modulator cannot lock.
- The output frequency in the GQAM modulator may be incorrect.

Note: The RF output field on the front panel LCD screen displays “MUTED” when this condition exists.

Check and Correct

The PLL synthesizer cannot lock or the output frequency is no correct

- 1 Power down and then power up the GQAM modulator using the on/off rocker-type switch on the back panel, or reset the GQAM modulator from the EC.
- 2 Replace the GQAM modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the GQAM modulator.
- 3 Contact Cisco Services for further assistance.

GQAM Modulator Alarm ID 7 (7 Hex)

The **RF1 Calibration Error** alarm occurs when the RF level settings at RF OUT 1 in the GQAM modulator are not calibrated to the correct frequency or when the EEPROM that stores the calibration data is not operational. When this condition exists, there is potential loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the GQAM modulator that is sending this alarm.

Front Panel Message

RF1 Level not calibrated

Possible Cause(s)

- The RF level settings at RF OUT 1 in the GQAM modulator are not calibrated to the correct frequency.
- The EEPROM that stores the calibration data for the GQAM modulator is not operational.

Check and Correct

- 1 Power down and then power up the GQAM modulator using the on/off rocker-type switch on the back panel, or reset the GQAM modulator from the EC.
- 2 Replace the GQAM modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the GQAM modulator.
- 3 If the alarm continues to occur, contact Cisco Services for further assistance.

GQAM Modulator Alarm ID 8 (8 Hex)

The **RF1 UC Lock Detect Error** alarm occurs when the UC PLL lock detect signal at RF OUT 1 in the GQAM modulator is functioning incorrectly. There is no RF output at RF OUT 1 when this condition exists, and therefore no services are available through the RF OUT 1 port.

Front Panel Message

RF1 UC Lock detect error

Possible Cause(s)

The UC PLL lock detect signal at RF OUT 1 in the GQAM modulator is functioning incorrectly.

Note: The RF output field on the front panel screen displays “MUTED” when this condition exists.

Check and Correct

- 1 Power down and then power up the GQAM modulator using the on/off rocker-type switch on the back panel, or reset the GQAM modulator from the EC.
- 2 If resetting the GQAM modulator does not solve the problem, contact Cisco Services for further assistance.

GQAM Modulator Alarm ID 9 (9 Hex)

The **RF1 UC PLL Unlocked Error** alarm occurs when the UC PLL at RF OUT 1 in the GQAM modulator is unlocked. There is no RF output at RF OUT 1 when this condition exists, and therefore no services are available through the RF OUT 1 port.

Front Panel Message

RF1 UC PLL unlocked

Possible Cause(s)

- The UC PLL at RF OUT 1 in the GQAM modulator is unlocked.
- The output frequency transmitted from the GQAM modulator may be incorrect.
Note: The RF output field on the front panel screen displays “MUTED” when this condition exists.

Check and Correct

- 1 Power down and then power up the GQAM modulator using the on/off rocker-type switch on the back panel, or reset the GQAM modulator from the EC.
- 2 If resetting the GQAM modulator does not solve the problem, contact Cisco Services for further assistance.

GQAM Modulator Alarm ID 10 (A Hex)

The **RF1 EEPROM Failure** alarm occurs when the EEPROM at RF OUT 1 in the GQAM modulator is not present or is not operational. No services or poor quality services are available through the RF OUT 1 port.

The following conditions also exist when this alarm occurs:

- RF calibration data is not available.
- The **GQAM Modulator RF (1-4) Calibration Error** alarm is active.
- The **RF (1-4) Level not calibrated** alarm message appears on the front panel LCD screen.

Front Panel Message

RF1 EEPROM failure

Possible Cause(s)

The EEPROM in the GQAM modulator at RF OUT 1 failed, is not present, or is not operational.

Check and Correct

- 1 Power down and then power up the GQAM modulator using the on/off rocker-type switch on the back panel, or reset the GQAM modulator from the EC.
- 2 Replace the GQAM modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the GQAM modulator.
- 3 Contact Cisco Services for further assistance.

GQAM Modulator Alarm ID 11 (B Hex)

The **RF2 Communication Error** alarm occurs when the digital I/O board in the GQAM modulator cannot communicate with the RF MCU at RF OUT 2 . When this alarm occurs, video is not transmitted through the RF OUT 2 port.

Front Panel Message

RF2 Comm. failure

Possible Cause(s)

- The digital I/O board cannot communicate with the MCU on the GQAM modulator RF board at RF OUT 2.
- The MCU at RF OUT 2 on the GQAM modulator is not programmed correctly.
- The CRC checksum error did not clear correctly.
- The power supply failed or is failing.

Check and Correct

Digital I/O board cannot communicate with the MCU

Check for loose connections or defective cables, tighten any loose cables, and replace any defective cables.

MCU not programmed correctly

- 1 Power down and then power up the GQAM modulator using the on/off rocker-type switch on the back panel, or reset the GQAM modulator from the EC.
- 2 If resetting the GQAM modulator does not correct the problem, contact Cisco Services.

CRC checksum error

CRC errors are transient and intermittent and clear automatically.

Power supply failure

Replace the GQAM modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the GQAM modulator.

GQAM Modulator Alarm ID 12 (C Hex)

The **RF2 Excessive Temperature** alarm occurs when the internal temperature of the GQAM modulator exceeds 70°C (158°F). A GQAM modulator that is overheating could have minimal to severe impact on services. If the modulator fails due to overheating, there would be no services available from that GQAM modulator.

Front Panel Message

RF2 Exceeded max temp

Possible Cause(s)

- The vents on the GQAM modulator are blocked.
- The room temperature is too high.
- A fan failure occurred.
- A hardware failure occurred.

Check and Correct

Vents are blocked

Check and clear any obstructions from the vents.

Room temperature is too high

Check and repair or replace the heating/cooling equipment in the room.

Fan failure

Check and repair or replace the fan.

Hardware failure

- 1 Replace the GQAM modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the GQAM modulator.
- 2 If the alarm condition continues to occur, Contact Cisco Services.

GQAM Modulator Alarm ID 13 (D Hex)

The **RF2 Power Supply Failure** alarm occurs when at least one internal power supply in the GQAM modulator fails. There is no RF output at RF OUT 2 when this condition exists, and video is not transmitted through the RF OUT 2 port. This condition could also generate a communication alarm. No services are available through the RF OUT 2 port.

Front Panel Message

RF2 Power supply failure

Possible Cause(s)

The internal power supply to RF OUT 2 in the GQAM modulator has failed or is failing.

Note: The RF output field on the front panel LCD screen displays “MUTED” when this condition exists.

Check and Correct

- 1 Check power source, power wires, and the on/off rocker-type switch on the back panel of the GQAM modulator.
- 2 Replace the GQAM modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the GQAM modulator.
- 3 Contact Cisco Services for further assistance.

GQAM Modulator Alarm ID 14 (E Hex)

The **RF2 DC Lock Detect Error** alarm occurs when the DC lock detect signal at RF OUT 2 in the GQAM modulator is functioning incorrectly. There is no RF output at RF OUT 2 when this condition exists, and video is not transmitted through the RF OUT 2 port.

Front Panel Message

RF2 DC Lock detect error

Possible Cause(s)

- The DC lock detect signal at RF OUT 2 in the GQAM modulator is functioning incorrectly.
- During the MCU POST, the lock detect signal from the DC PLL at RF OUT 2 in the GQAM modulator did not indicate an unlocked condition when one existed.
- The output converter synthesizer in the GQAM modulator has malfunctioned.
Note: The RF output field on the front panel LCD screen displays “MUTED” when this condition exists.

Check and Correct

- 1 Power down and then power up the GQAM modulator using the on/off rocker-type switch on the back panel, or reset the GQAM modulator from the EC.
- 2 Replace the GQAM modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing and repairing the GQAM modulator.
- 3 Contact Cisco Services for further assistance.

GQAM Modulator Alarm ID 15 (F Hex)

The **RF2 DC PLL Unlocked Error** alarm occurs when the DC PLL synthesizer at RF OUT 2 in the GQAM modulator cannot lock. There is no RF output at RF OUT 2 when this condition exists because the signal is not synchronized, and video is not transmitted through the RF OUT 2 port.

Front Panel Message

RF2 DC PLL unlocked

Possible Cause(s)

- The DC PLL synthesizer at RF OUT 2 in the GQAM modulator cannot lock.
- The output frequency in the GQAM modulator may be incorrect.

Note: The RF output field on the front panel LCD screen displays “MUTED” when this condition exists.

Check and Correct

The PLL synthesizer cannot lock or the output frequency is no correct

- 1 Power down and then power up the GQAM modulator using the on/off rocker-type switch on the back panel, or reset the GQAM modulator from the EC.
- 2 Replace the GQAM modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the GQAM modulator.
- 3 Contact Cisco Services for further assistance.

GQAM Modulator Alarm ID 17 (11 Hex)

The **RF2 Calibration Error** alarm occurs when the RF level settings at RF OUT 2 in the GQAM modulator are not calibrated to the correct frequency or when the EEPROM that stores the calibration data is not operational. When this condition exists, there is potential loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the GQAM modulator that is sending this alarm.

Front Panel Message

RF2 Level not calibrated

Possible Cause(s)

- The RF level settings at RF OUT 2 in the GQAM modulator are not calibrated to the correct frequency.
- The EEPROM that stores the calibration data for the GQAM modulator is not operational.

Check and Correct

- 1 Power down and then power up the GQAM modulator using the on/off rocker-type switch on the back panel, or reset the GQAM modulator from the EC.
- 2 Replace the GQAM modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the GQAM modulator.
- 3 If the alarm continues to occur, contact Cisco Services for further assistance.

GQAM Modulator Alarm ID 18 (12 Hex)

The **RF2 UC Lock Detect Error** alarm occurs when the UC PLL lock detect signal at RF OUT 2 in the GQAM modulator is functioning incorrectly. There is no RF output at RF OUT 2 when this condition exists, and therefore no services are available through the RF OUT 2 port.

Front Panel Message

RF2 UC Lock detect error

Possible Cause(s)

The UC PLL lock detect signal at RF OUT 2 in the GQAM modulator is functioning incorrectly.

Note: The RF output field on the front panel screen displays “MUTED” when this condition exists.

Check and Correct

- 1 Power down and then power up the GQAM modulator using the on/off rocker-type switch on the back panel, or reset the GQAM modulator from the EC.
- 2 If resetting the GQAM modulator does not solve the problem, contact Cisco Services for further assistance.

GQAM Modulator Alarm ID 19 (13 Hex)

The **RF2 UC PLL Unlocked Error** alarm occurs when the UC PLL at RF OUT 2 in the GQAM modulator is unlocked. There is no RF output at RF OUT 2 when this condition exists, and therefore no services are available through the RF OUT 2 port.

Front Panel Message

RF2 UC PLL unlocked

Possible Cause(s)

- The UC PLL at RF OUT 2 in the GQAM modulator is unlocked.
- The output frequency transmitted from the GQAM modulator may be incorrect.
Note: The RF output field on the front panel screen displays “MUTED” when this condition exists.

Check and Correct

- 1 Power down and then power up the GQAM modulator using the on/off rocker-type switch on the back panel, or reset the GQAM modulator from the EC.
- 2 If resetting the GQAM modulator does not solve the problem, contact Cisco Services for further assistance.

GQAM Modulator Alarm ID 20 (14 Hex)

The **RF2 EEPROM Failure** alarm occurs when the EEPROM at RF OUT 2 in the GQAM modulator is not present or is not operational. No services or poor quality services are available through the RF OUT 2 port.

The following conditions also exist when this alarm occurs:

- RF calibration data is not available.
- The **GQAM Modulator RF (1-4) Calibration Error** alarm is active.
- The **RF (1-4) Level not calibrated** alarm message appears on the front panel LCD screen.

Front Panel Message

RF2 EEPROM failure

Possible Cause(s)

The EEPROM in the GQAM modulator at RF OUT 2 failed, is not present, or is not operational.

Check and Correct

- 1 Power down and then power up the GQAM modulator using the on/off rocker-type switch on the back panel, or reset the GQAM modulator from the EC.
- 2 Replace the GQAM modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the GQAM modulator.
- 3 Contact Cisco Services for further assistance.

GQAM Modulator Alarm ID 21 (15 Hex)

The **RF3 Communication Error** alarm occurs when the digital I/O board in the GQAM modulator cannot communicate with the RF MCU at RF OUT 3. When this alarm occurs, video is not transmitted through the RF OUT 3 port.

Front Panel Message

RF3 Comm. failure

Possible Cause(s)

- The digital I/O board cannot communicate with the MCU on the GQAM modulator RF board at RF OUT 3.
- The MCU at RF OUT 3 on the GQAM modulator is not programmed correctly.
- The CRC checksum error did not clear correctly.
- The power supply failed or is failing.

Check and Correct

Digital I/O board cannot communicate with the MCU

Check for loose connections or defective cables, tighten any loose cables, and replace any defective cables.

MCU not programmed correctly

- 1 Power down and then power up the GQAM modulator using the on/off rocker-type switch on the back panel, or reset the GQAM modulator from the EC.
- 2 If resetting the GQAM modulator does not correct the problem, contact Cisco Services.

CRC checksum error

CRC errors are transient and intermittent and clear automatically.

Power supply failure

Replace the GQAM modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the GQAM modulator.

GQAM Modulator Alarm ID 22 (16 Hex)

The **RF3 Excessive Temperature** alarm occurs when the internal temperature of the GQAM modulator exceeds 70°C (158°F). A GQAM modulator that is overheating could have minimal to severe impact on services. If the modulator fails due to overheating, there would be no services available from that GQAM modulator.

Front Panel Message

RF3 Exceeded max temp

Possible Cause(s)

- The vents on the GQAM modulator are blocked.
- The room temperature is too high.
- A fan failure occurred.
- A hardware failure occurred.

Check and Correct

Vents are blocked

Check and clear any obstructions from the vents.

Room temperature is too high

Check and repair or replace the heating/cooling equipment in the room.

Fan failure

Check and repair or replace the fan.

Hardware failure

- 1 Replace the GQAM modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the GQAM modulator.
- 2 If the alarm condition continues to occur, contact Cisco Services.

GQAM Modulator Alarm ID 23 (17 Hex)

The **RF3 Power Supply Failure** alarm occurs when at least one internal power supply in the GQAM modulator fails. There is no RF output at RF OUT 3 when this condition exists, and video is not transmitted through the RF OUT 3 port. This condition could also generate a communication alarm. No services are available through the RF OUT 3 port.

Front Panel Message

RF3 Power supply failure

Possible Cause(s)

The internal power supply to RF OUT 3 in the GQAM modulator has failed or is failing.

Note: The RF output field on the front panel LCD screen displays “MUTED” when this condition exists.

Check and Correct

- 1 Check power source, power wires, and the on/off rocker-type switch on the back panel of the GQAM modulator.
- 2 Replace the GQAM modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the GQAM modulator.
- 3 Contact Cisco Services for further assistance.

GQAM Modulator Alarm ID 24 (18 Hex)

The **RF3 DC Lock Detect Error** alarm occurs when the DC lock detect signal at RF OUT 3 in the GQAM modulator is functioning incorrectly. There is no RF output at RF OUT 3 when this condition exists, and video is not transmitted through the RF OUT 3 port.

Front Panel Message

RF3 DC Lock detect error

Possible Cause(s)

- The DC lock detect signal at RF OUT 3 in the GQAM modulator is functioning incorrectly.
- During the MCU POST, the lock detect signal from the DC PLL at RF OUT 3 in the GQAM modulator did not indicate an unlocked condition when one existed.
- The output converter synthesizer in the GQAM modulator has malfunctioned.
Note: The RF output field on the front panel LCD screen displays “MUTED” when this condition exists.

Check and Correct

- 1 Power down and then power up the GQAM modulator using the on/off rocker-type switch on the back panel, or reset the GQAM modulator from the EC.
- 2 Replace the GQAM modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the GQAM modulator.
- 3 Contact Cisco Services for further assistance.

GQAM Modulator Alarm ID 25 (19 Hex)

The **RF3 DC PLL Unlocked Error** alarm occurs when the DC PLL synthesizer at RF OUT 3 in the GQAM modulator cannot lock. There is no RF output at RF OUT 3 when this condition exists because the signal is not synchronized, and video is not transmitted through the RF OUT 3 port.

Front Panel Message

RF3 DC PLL unlocked

Possible Cause(s)

- The DC PLL synthesizer at RF OUT 3 in the GQAM modulator cannot lock.
- The output frequency in the GQAM modulator may be incorrect.

Note: The RF output field on the front panel LCD screen displays “MUTED” when this condition exists.

Check and Correct

The PLL synthesizer cannot lock or the output frequency is no correct

- 1 Power down and then power up the GQAM modulator using the on/off rocker-type switch on the back panel, or reset the GQAM modulator from the EC.
- 2 Replace the GQAM modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the GQAM modulator.
- 3 Contact Cisco Services for further assistance.

GQAM Modulator Alarm ID 27 (1B Hex)

The **RF3 Calibration Error** alarm occurs when the RF level settings at RF OUT 3 in the GQAM modulator are not calibrated to the correct frequency or when the EEPROM that stores the calibration data is not operational. When this condition exists, there is potential loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the GQAM modulator that is sending this alarm.

Front Panel Message

RF3 Level not calibrated

Possible Cause(s)

- The RF level settings at RF OUT 3 in the GQAM modulator are not calibrated to the correct frequency.
- The EEPROM that stores the calibration data for the GQAM modulator is not operational.

Check and Correct

- 1 Power down and then power up the GQAM modulator using the on/off rocker-type switch on the back panel, or reset the GQAM modulator from the EC.
- 2 Replace the GQAM modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the GQAM modulator.
- 3 If the alarm continues to occur, contact Cisco Services for further assistance.

GQAM Modulator Alarm ID 28 (1C Hex)

The **RF3 UC Lock Detect Error** alarm occurs when the UC PLL lock detect signal at RF OUT 3 in the GQAM modulator is functioning incorrectly. There is no RF output at RF OUT 3 when this condition exists, and therefore no services are available through the RF OUT 3 port.

Front Panel Message

RF3 UC Lock detect error

Possible Cause(s)

The UC PLL lock detect signal at RF OUT 3 in the GQAM modulator is functioning incorrectly.

Note: The RF output field on the front panel screen displays “MUTED” when this condition exists.

Check and Correct

- 1 Power down and then power up the GQAM modulator using the on/off rocker-type switch on the back panel, or reset the GQAM modulator from the EC.
- 2 If resetting the GQAM modulator does not solve the problem, contact Cisco Services for further assistance.

GQAM Modulator Alarm ID 29 (1D Hex)

The **RF3 UC PLL Unlocked Error** alarm occurs when the UC PLL at RF OUT 3 in the GQAM modulator is unlocked. There is no RF output at RF OUT 3 when this condition exists, and therefore no services are available through the RF OUT 3 port.

Front Panel Message

RF3 UC PLL unlocked

Possible Cause(s)

- The UC PLL at RF OUT 3 in the GQAM modulator is unlocked.
- The output frequency transmitted from the GQAM modulator may be incorrect.
Note: The RF output field on the front panel screen displays “MUTED” when this condition exists.

Check and Correct

- 1 Power down and then power up the GQAM modulator using the on/off rocker-type switch on the back panel, or reset the GQAM modulator from the EC.
- 2 If resetting the GQAM modulator does not solve the problem, contact Cisco Services for further assistance.

GQAM Modulator Alarm ID 30 (1E Hex)

The **RF3 EEPROM Failure** alarm occurs when the EEPROM at RF OUT 3 in the GQAM modulator is not present or is not operational. No services or poor quality services are available through the RF OUT 3 port.

The following conditions also exist when this alarm occurs:

- RF calibration data is not available.
- The **GQAM Modulator RF (1-4) Calibration Error** alarm is active.
- The **RF (1-4) Level not calibrated** alarm message appears on the front panel LCD screen.

Front Panel Message

RF3 EEPROM failure

Possible Cause(s)

The EEPROM in the GQAM modulator at RF OUT 3 failed, is not present, or is not operational.

Check and Correct

- 1 Power down and then power up the GQAM modulator using the on/off rocker-type switch on the back panel, or reset the GQAM modulator from the EC.
- 2 Replace the GQAM modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the GQAM modulator.
- 3 Contact Cisco Services for further assistance.

GQAM Modulator Alarm ID 31 (1F Hex)

The **RF4 Communication Error** alarm occurs when the digital I/O board in the GQAM modulator cannot communicate with the RF MCU at RF OUT 4. When this alarm occurs, video is not transmitted through the RF OUT 4 port.

Front Panel Message

RF4 Comm. failure

Possible Cause(s)

- The digital I/O board cannot communicate with the MCU on the GQAM modulator RF board at RF OUT 4.
- The MCU at RF OUT 4 on the GQAM modulator is not programmed correctly.
- The CRC checksum error did not clear correctly.
- The power supply failed or is failing.

Check and Correct

Digital I/O board cannot communicate with the MCU

Check for loose connections or defective cables, tighten any loose cables, and replace any defective cables.

MCU not programmed correctly

- 1 Power down and then power up the GQAM modulator using the on/off rocker-type switch on the back panel, or reset the GQAM modulator from the EC.
- 2 If resetting the GQAM modulator does not correct the problem, contact Cisco Services.

CRC checksum error

CRC errors are transient and intermittent and clear automatically.

Power supply failure

Replace the GQAM modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the GQAM modulator.

GQAM Modulator Alarm ID 32 (20 Hex)

The **RF4 Excessive Temperature** alarm occurs when the internal temperature of the GQAM modulator exceeds 70°C (158°F). A GQAM modulator that is overheating could have minimal to severe impact on services. If the modulator fails due to overheating, there would be no services available from that GQAM modulator.

Front Panel Message

RF4 Exceeded max temp

Possible Cause(s)

- The vents on the GQAM modulator are blocked.
- The room temperature is too high.
- A fan failure occurred.
- A hardware failure occurred.

Check and Correct

Vents are blocked

Check and clear any obstructions from the vents.

Room temperature is too high

Check and repair or replace the heating/cooling equipment in the room.

Fan failure

Check and repair or replace the fan.

Hardware failure

- 1 Replace the GQAM modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the GQAM modulator.
- 2 If the alarm condition continues to occur, contact Cisco Services.

GQAM Modulator Alarm ID 33 (21 Hex)

The **RF4 Power Supply Failure** alarm occurs when at least one internal power supply in the GQAM modulator fails. There is no RF output at RF OUT 4 when this condition exists, and video is not transmitted through the RF OUT 4 port. This condition could also generate a communication alarm. No services are available through the RF OUT 4 port.

Front Panel Message

RF4 Power supply failure

Possible Cause(s)

The internal power supply to RF OUT 4 in the GQAM modulator has failed or is failing.

Note: The RF output field on the front panel LCD screen displays “MUTED” when this condition exists.

Check and Correct

- 1 Check power source, power wires, and the on/off rocker-type switch on the back panel of the GQAM modulator.
- 2 Replace the GQAM modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the GQAM modulator.
- 3 Contact Cisco Services for further assistance.

GQAM Modulator Alarm ID 34 (22 Hex)

The **RF4 DC Lock Detect Error** alarm occurs when the DC lock detect signal at RF OUT 4 in the GQAM modulator is functioning incorrectly. There is no RF output at RF OUT 4 when this condition exists, and video is not transmitted through the RF OUT 4 port.

Front Panel Message

RF4 DC Lock detect error

Possible Cause(s)

- The DC lock detect signal at RF OUT 4 in the GQAM modulator is functioning incorrectly.
- During the MCU POST, the lock detect signal from the DC PLL at RF OUT 4 in the GQAM modulator did not indicate an unlocked condition when one existed.
- The output converter synthesizer in the GQAM modulator has malfunctioned.
Note: The RF output field on the front panel LCD screen displays “MUTED” when this condition exists.

Check and Correct

- 1 Power down and then power up the GQAM modulator using the on/off rocker-type switch on the back panel, or reset the GQAM modulator from the EC.
- 2 Replace the GQAM modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the GQAM modulator.
- 3 Contact Cisco Services for further assistance.

GQAM Modulator Alarm ID 35 (23 Hex)

The **RF4 DC PLL Unlocked Error** alarm occurs when the DC PLL synthesizer at RF OUT 4 in the GQAM modulator cannot lock. There is no RF output at RF OUT 4 when this condition exists because the signal is not synchronized, and video is not transmitted through the RF OUT 4 port.

Front Panel Message

RF4 DC PLL unlocked

Possible Cause(s)

- The DC PLL synthesizer at RF OUT 4 in the GQAM modulator cannot lock.
- The output frequency in the GQAM modulator may be incorrect.

Note: The RF output field on the front panel LCD screen displays “MUTED” when this condition exists.

Check and Correct

The PLL synthesizer cannot lock or the output frequency is no correct

- 1 Power down and then power up the GQAM modulator using the on/off rocker-type switch on the back panel, or reset the GQAM modulator from the EC.
- 2 Replace the GQAM modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the GQAM modulator.
- 3 Contact Cisco Services for further assistance.

GQAM Modulator Alarm ID 37 (25 Hex)

The **RF4 Calibration Error** alarm occurs when the RF level settings at RF OUT 4 in the GQAM modulator are not calibrated to the correct frequency or when the EEPROM that stores the calibration data is not operational. When this condition exists, there is potential loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the GQAM modulator that is sending this alarm.

Front Panel Message

RF4 Level not calibrated

Possible Cause(s)

- The RF level settings at RF OUT 4 in the GQAM modulator are not calibrated to the correct frequency.
- The EEPROM that stores the calibration data for the GQAM modulator is not operational.

Check and Correct

- 1 Power down and then power up the GQAM modulator using the on/off rocker-type switch on the back panel, or reset the GQAM modulator from the EC.
- 2 Replace the GQAM modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the GQAM modulator.
- 3 If the alarm continues to occur, contact Cisco Services for further assistance.

GQAM Modulator Alarm ID 38 (26 Hex)

The **RF4 UC Lock Detect Error** alarm occurs when the UC PLL lock detect signal at RF OUT 4 in the GQAM modulator is functioning incorrectly. There is no RF output at RF OUT 4 when this condition exists, and therefore no services are available through the RF OUT 4 port.

Front Panel Message

RF4 UC Lock detect error

Possible Cause(s)

The UC PLL lock detect signal at RF OUT 4 in the GQAM modulator is functioning incorrectly.

Note: The RF output field on the front panel screen displays “MUTED” when this condition exists.

Check and Correct

- 1 Power down and then power up the GQAM modulator using the on/off rocker-type switch on the back panel, or reset the GQAM modulator from the EC.
- 2 If resetting the GQAM modulator does not solve the problem, contact Cisco Services for further assistance.

GQAM Modulator Alarm ID 39 (27 Hex)

The **RF4 UC PLL Unlocked Error** alarm occurs when the UC PLL at RF OUT 4 in the GQAM modulator is unlocked. There is no RF output at RF OUT 4 when this condition exists, and therefore no services are available through the RF OUT 4 port.

Front Panel Message

RF4 UC PLL unlocked

Possible Cause(s)

- The UC PLL at RF OUT 4 in the GQAM modulator is unlocked.
- The output frequency transmitted from the GQAM modulator may be incorrect.
Note: The RF output field on the front panel LCD screen displays “MUTED” when this condition exists.

Check and Correct

- 1 Power down and then power up the GQAM modulator using the on/off rocker-type switch on the back panel, or reset the GQAM modulator from the EC.
- 2 If resetting the GQAM modulator does not solve the problem, contact Cisco Services for further assistance.

GQAM Modulator Alarm ID 40 (28 Hex)

The **RF4 EEPROM Failure** alarm occurs when the EEPROM at RF OUT 4 in the GQAM modulator is not present or is not operational. No services or poor quality services are available through the RF OUT 4 port.

The following conditions also exist when this alarm occurs:

- RF calibration data is not available.
- The **GQAM Modulator RF (1-4) Calibration Error** alarm is active.
- The **RF (1-4) Level not calibrated** alarm message appears on the front panel LCD screen.

Front Panel Message

RF4 EEPROM failure

Possible Cause(s)

The EEPROM in the GQAM modulator at RF OUT 4 failed, is not present, or is not operational.

Check and Correct

- 1 Power down and then power up the GQAM modulator using the on/off rocker-type switch on the back panel, or reset the GQAM modulator from the EC.
- 2 Replace the GQAM modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the GQAM modulator.
- 3 Contact Cisco Services for further assistance.

GQAM Modulator Alarm ID 41 (29 Hex)

The **Reset Detected** status event occurs during the boot-up process or when the GQAM modulator is reset by either a loss of power or a manual reset. There is a potential for loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the GQAM modulator that is sending this event until it returns for full service.

Front Panel Message

Reset detected

Possible Cause(s)

- The GQAM modulator is rebooting.
- A user or system operator reset the GQAM modulator.
- A loss of power occurred.
- There is a problem in the DBDS.

Check and Correct

Session and provisioning data are sent to the GQAM modulator again by the EC. However, you should also check the following:

- 1 Verify that there are still broadcast services on this GQAM modulator.
- 2 Verify that the reset did not adversely affect broadcast services.
- 3 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 4 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 5 Contact Cisco Services for further assistance.

GQAM Modulator Alarm ID 42 (2A Hex)

The **Input 1 MPEG Continuity Error** alarm can occur when individual MPEG packets become corrupted due to random noise in the network. Each MPEG packet has a section for continuity bits that should contain a sequential value. These MPEG continuity bits are used by the MPEG packet recipient to verify that the packets in an MPEG stream are received in the correct sequential order and to verify that no packet loss has occurred.

This alarm also occurs when the GQAM modulator receives packets in the MPEG stream that do not contain MPEG continuity bits.

There is a potential for loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the GQAM modulator that is sending this alarm.

Notes:

- This alarm may also occur and clear when the ASI cable is disconnected and then reconnected.
- This alarm is self-clearing and may be intermittent due to random noise in the system. Single instances of this alarm that clear automatically and that do not reappear are not a cause for concern.

Front Panel Message

Input 1 MPEG Continuity Error

Possible Cause(s)

- A cable is loose, disconnected, or defective.
- There are data errors on the satellite link.
- The rate of change of the IEC exceeds the allowed threshold.
- There is defective upstream equipment or failure on the input data link of the GQAM modulator.
- There is defective local MPEG coding.
- The GQAM modulator is defective.

Check and Correct

Loose, disconnected, or defective cables

Check for loose connections or defective cables, tighten any loose cable connections, connect any disconnected cables, and replace any defective cables.

Chapter 3 GQAM Modulator Alarms

Satellite link data errors

Contact your signal provider to verify if there are any problems with their satellite transmissions.

IEC errors

Clean up the MPEG signal input to the GQAM modulator by checking the IRT, RTE, and MPEG encoder.

Defective upstream equipment

- 1 Check the upstream devices that are sending MPEG packets to the GQAM modulator.
- 2 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of service.

Important!

- If the majority of MPEG packet alarms are occurring in a single GQAM modulator, then that GQAM modulator or its input should be the focus of the troubleshooting.
 - If the majority of MPEG packet alarms are occurring in more than one GQAM modulator, then the troubleshooting should focus upstream on the device that is providing a common source of input to the GQAM modulators with errors.
 - If the GQAM modulators all have a common device upstream, then that device is the most likely source of the packet errors
- 3 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
 - 4 If the alarm continues to occur, contact Cisco Services for further assistance.

Defective local MPEG coding

Check the local source devices that are providing MPEG content to the GQAM modulator.

GQAM modulator defective

- 1 Replace the GQAM modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the GQAM modulator.
- 2 If the alarm continues to occur, contact Cisco Services for further assistance.

GQAM Modulator Alarm ID 43 (2B Hex)

The **Input 1 MPEG Transport Error** alarm occurs when there is an error in the header of some of the MPEG packets received by the GQAM modulator. There is a potential for loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the GQAM modulator that is sending this alarm.

Note: This alarm is self-clearing and may be intermittent. Single instances of this alarm that clear automatically and that do not reappear are not a cause for concern.

Front Panel Message

Input 1 MPEG Transport error

Possible Cause(s)

There is an error in the header of an MPEG packet.

Check and Correct

- 1 Check the upstream devices that are sending MPEG packets to the ASI input ports on the GQAM modulator.
- 2 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 3 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 4 If the alarm continues to occur, contact Cisco Services for further assistance.

GQAM Modulator Alarm ID 44 (2C Hex)

The **Input 2 MPEG Continuity Error** alarm can occur when individual MPEG packets become corrupted due to random noise in the network. Each MPEG packet has a section for continuity bits that should contain a sequential value. These MPEG continuity bits are used by the MPEG packet recipient to verify that the packets in an MPEG stream are received in the correct sequential order and to verify that no packet loss has occurred.

This alarm also occurs when the GQAM modulator receives packets in the MPEG stream that do not contain MPEG continuity bits.

There is a potential for loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the GQAM modulator that is sending this alarm.

Notes:

- This alarm may also occur and clear when the ASI cable is disconnected and then reconnected.
- This alarm is self-clearing and may be intermittent due to random noise in the system. Single instances of this alarm that clear automatically and that do not reappear are not a cause for concern.

Front Panel Message

Input 2 MPEG Continuity Error

Possible Cause(s)

- A cable is loose, disconnected, or defective.
- There are data errors on the satellite link.
- The rate of change of the IEC exceeds the allowed threshold.
- There is defective upstream equipment or failure on the input data link of the GQAM modulator.
- There is defective local MPEG coding.
- The GQAM modulator is defective.

Check and Correct

Loose, disconnected, or defective cables

Check for loose connections or defective cables, tighten any loose cable connections, connect any disconnected cables, and replace any defective cables.

Satellite link data errors

Contact your signal provider to verify if there are any problems with their satellite transmissions.

IEC errors

Clean up the MPEG signal input to the GQAM modulator by checking the IRT, RTE, and MPEG encoder.

Defective upstream equipment

- 1 Check the upstream devices that are sending MPEG packets to the GQAM modulator.
- 2 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of service.

Important!

- If the majority of MPEG packet alarms are occurring in a single GQAM modulator, then that GQAM modulator or its input should be the focus of the troubleshooting.
 - If the majority of MPEG packet alarms are occurring in more than one GQAM modulator, then the troubleshooting should focus upstream on the device that is providing a common source of input to the GQAM modulators with errors.
 - If the GQAM modulators all have a common device upstream, then that device is the most likely source of the packet errors.
- 3 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
 - 4 If the alarm continues to occur, contact Cisco Services for further assistance.

Defective local MPEG coding

Check the local source devices that are providing MPEG content to the GQAM modulator.

GQAM modulator defective

- 1 Replace the GQAM modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the GQAM modulator.
- 2 If the alarm continues to occur, contact Cisco Services for further assistance.

GQAM Modulator Alarm ID 45 (2D Hex)

The **Input 2 MPEG Transport Error** alarm occurs when there is an error in the header of some of the MPEG packets received by the GQAM modulator. There is a potential for loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the GQAM modulator that is sending this alarm.

Note: This alarm is self-clearing and may be intermittent. Single instances of this alarm that clear automatically and that do not reappear are not a cause for concern.

Front Panel Message

Input 2 MPEG Transport error

Possible Cause(s)

There is an error in the header of an MPEG packet.

Check and Correct

- 1 Check the upstream devices that are sending MPEG packets to the ASI input ports on the GQAM modulator.
- 2 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 3 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 4 If the alarm continues to occur, contact Cisco Services for further assistance.

GQAM Modulator Alarm ID 46 (2E Hex)

The **Input 3 MPEG Continuity Error** alarm can occur when individual MPEG packets become corrupted due to random noise in the network. Each MPEG packet has a section for continuity bits that should contain a sequential value. These MPEG continuity bits are used by the MPEG packet recipient to verify that the packets in an MPEG stream are received in the correct sequential order and to verify that no packet loss has occurred.

This alarm also occurs when the GQAM modulator receives packets in the MPEG stream that do not contain MPEG continuity bits.

There is a potential for loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the GQAM modulator that is sending this alarm.

Notes:

- This alarm may also occur and clear when the ASI cable is disconnected and then reconnected.
- This alarm is self-clearing and may be intermittent due to random noise in the system. Single instances of this alarm that clear automatically and that do not reappear are not a cause for concern.

Front Panel Message

Input 3 MPEG Continuity Error

Possible Cause(s)

- A cable is loose, disconnected, or defective.
- There are data errors on the satellite link.
- The rate of change of the IEC exceeds the allowed threshold.
- There is defective upstream equipment or failure on the input data link of the GQAM modulator.
- There is defective local MPEG coding.
- The GQAM modulator is defective.

Check and Correct

Loose, disconnected, or defective cables

Check for loose connections or defective cables, tighten any loose cable connections, connect any disconnected cables, and replace any defective cables.

Chapter 3 GQAM Modulator Alarms

Satellite link data errors

Contact your signal provider to verify if there are any problems with their satellite transmissions.

IEC errors

Clean up the MPEG signal input to the GQAM modulator by checking the IRT, RTE, and MPEG encoder.

Defective upstream equipment

- 1 Check the upstream devices that are sending MPEG packets to the GQAM modulator.
- 2 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of service.

Important!

- If the majority of MPEG packet alarms are occurring in a single GQAM modulator, then that GQAM modulator or its input should be the focus of the troubleshooting.
 - If the majority of MPEG packet alarms are occurring in more than one GQAM modulator, then the troubleshooting should focus upstream on the device that is providing a common source of input to the GQAM modulators with errors.
 - If the GQAM modulators all have a common device upstream, then that device is the most likely source of the packet errors
- 3 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
 - 4 If the alarm continues to occur, contact Cisco Services for further assistance.

Defective local MPEG coding

Check the local source devices that are providing MPEG content to the GQAM modulator.

GQAM modulator defective

- 1 Replace the GQAM modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the GQAM modulator.
- 2 If the alarm continues to occur, contact Cisco Services for further assistance.

GQAM Modulator Alarm ID 47 (2F Hex)

The **Input 3 MPEG Transport Error** alarm occurs when there is an error in the header of some of the MPEG packets received by the GQAM modulator. There is a potential for loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the GQAM modulator that is sending this alarm.

Note: This alarm is self-clearing and may be intermittent. Single instances of this alarm that clear automatically and that do not reappear are not a cause for concern.

Front Panel Message

Input 3 MPEG Transport error

Possible Cause(s)

There is an error in the header of an MPEG packet.

Check and Correct

- 1 Check the upstream devices that are sending MPEG packets to the ASI input ports on the GQAM modulator.
- 2 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 3 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 4 If the alarm continues to occur, contact Cisco Services for further assistance.

GQAM Modulator Alarm ID 48 (30 Hex)

The **Input 4 MPEG Continuity Error** alarm can occur when individual MPEG packets become corrupted due to random noise in the network. Each MPEG packet has a section for continuity bits that should contain a sequential value. These MPEG continuity bits are used by the MPEG packet recipient to verify that the packets in an MPEG stream are received in the correct sequential order and to verify that no packet loss has occurred.

This alarm also occurs when the GQAM modulator receives packets in the MPEG stream that do not contain MPEG continuity bits.

There is a potential for loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the GQAM modulator that is sending this alarm.

Notes:

- This alarm may also occur and clear when the ASI cable is disconnected and then reconnected.
- This alarm is self-clearing and may be intermittent due to random noise in the system. Single instances of this alarm that clear automatically and that do not reappear are not a cause for concern.

Front Panel Message

Input 4 MPEG Continuity Error

Possible Cause(s)

- A cable is loose, disconnected, or defective.
- There are data errors on the satellite link.
- The rate of change of the IEC exceeds the allowed threshold.
- There is defective upstream equipment or failure on the input data link of the GQAM modulator.
- There is defective local MPEG coding.
- The GQAM modulator is defective.

Check and Correct

Loose, disconnected, or defective cables

Check for loose connections or defective cables, tighten any loose cable connections, connect any disconnected cables, and replace any defective cables.

Satellite link data errors

Contact your signal provider to verify if there are any problems with their satellite transmissions.

IEC errors

Clean up the MPEG signal input to the GQAM modulator by checking the IRT, RTE, and MPEG encoder.

Defective upstream equipment

- 1 Check the upstream devices that are sending MPEG packets to the GQAM modulator.
- 2 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of service.

Important!

- If the majority of MPEG packet alarms are occurring in a single GQAM modulator, then that GQAM modulator or its input should be the focus of the troubleshooting.
 - If the majority of MPEG packet alarms are occurring in more than one GQAM modulator, then the troubleshooting should focus upstream on the device that is providing a common source of input to the GQAM modulators with errors.
 - If the GQAM modulators all have a common device upstream, then that device is the most likely source of the packet errors
- 3 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
 - 4 If the alarm continues to occur, contact Cisco Services for further assistance.

Defective local MPEG coding

Check the local source devices that are providing MPEG content to the GQAM modulator.

GQAM modulator defective

- 1 Replace the GQAM modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the GQAM modulator.
- 2 If the alarm continues to occur, contact Cisco Services for further assistance.

GQAM Modulator Alarm ID 49 (31 Hex)

The **Input 4 MPEG Transport Error** alarm occurs when there is an error in the header of some of the MPEG packets received by the GQAM modulator. There is a potential for loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the GQAM modulator that is sending this alarm.

Note: This alarm is self-clearing and may be intermittent. Single instances of this alarm that clear automatically and that do not reappear are not a cause for concern.

Front Panel Message

Input 4 MPEG Transport error

Possible Cause(s)

There is an error in the header of an MPEG packet.

Check and Correct

- 1 Check the upstream devices that are sending MPEG packets to the ASI input ports on the GQAM modulator.
- 2 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 3 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 4 If the alarm continues to occur, contact Cisco Services for further assistance.

GQAM Modulator Alarm ID 50 (32 Hex)

The **Input 5 MPEG Continuity Error** alarm can occur when individual MPEG packets become corrupted due to random noise in the network. Each MPEG packet has a section for continuity bits that should contain a sequential value. These MPEG continuity bits are used by the MPEG packet recipient to verify that the packets in an MPEG stream are received in the correct sequential order and to verify that no packet loss has occurred.

This alarm also occurs when the GQAM modulator receives packets in the MPEG stream that do not contain MPEG continuity bits.

There is a potential for loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the GQAM modulator that is sending this alarm.

Notes:

- This alarm may also occur and clear when the ASI cable is disconnected and then reconnected.
- This alarm is self-clearing and may be intermittent due to random noise in the system. Single instances of this alarm that clear automatically and that do not reappear are not a cause for concern.

Front Panel Message

Input 5 MPEG Continuity Error

Possible Cause(s)

- A cable is loose, disconnected, or defective.
- There are data errors on the satellite link.
- The rate of change of the IEC exceeds the allowed threshold.
- There is defective upstream equipment or failure on the input data link of the GQAM modulator.
- There is defective local MPEG coding.
- The GQAM modulator is defective.

Check and Correct

Loose, disconnected, or defective cables

Check for loose connections or defective cables, tighten any loose cable connections, connect any disconnected cables, and replace any defective cables.

Chapter 3 GQAM Modulator Alarms

Satellite link data errors

Contact your signal provider to verify if there are any problems with their satellite transmissions.

IEC errors

Clean up the MPEG signal input to the GQAM modulator by checking the IRT, RTE, and MPEG encoder.

Defective upstream equipment

- 1 Check the upstream devices that are sending MPEG packets to the GQAM modulator.
- 2 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of service.

Important!

- If the majority of MPEG packet alarms are occurring in a single GQAM modulator, then that GQAM modulator or its input should be the focus of the troubleshooting.
 - If the majority of MPEG packet alarms are occurring in more than one GQAM modulator, then the troubleshooting should focus upstream on the device that is providing a common source of input to the GQAM modulators with errors.
 - If the GQAM modulators all have a common device upstream, then that device is the most likely source of the packet errors
- 3 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
 - 4 If the alarm continues to occur, contact Cisco Services for further assistance.

Defective local MPEG coding

Check the local source devices that are providing MPEG content to the GQAM modulator.

GQAM modulator defective

- 1 Replace the GQAM modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the GQAM modulator.
- 2 If the alarm continues to occur, contact Cisco Services for further assistance.

GQAM Modulator Alarm ID 51 (33 Hex)

The **Input 5 MPEG Transport Error** alarm occurs when there is an error in the header of some of the MPEG packets received by the GQAM modulator. There is a potential for loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the GQAM modulator that is sending this alarm.

Note: This alarm is self-clearing and may be intermittent. Single instances of this alarm that clear automatically and that do not reappear are not a cause for concern.

Front Panel Message

Input 5 MPEG Transport error

Possible Cause(s)

There is an error in the header of an MPEG packet.

Check and Correct

- 1 Check the upstream devices that are sending MPEG packets to the GbE port on the GQAM modulator.
- 2 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 3 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 4 If the alarm continues to occur, contact Cisco Services for further assistance.

GQAM Modulator Alarm ID 52 (34 Hex)

The **Input 1 Loss of Signal Error** alarm occurs when there is no ASI signal to the ASI In 1 port in the GQAM modulator. Active program and data services that are present on ASI In 1 are not available.

Important! If you receive the loss of signal alarm an input that you are intentionally not using, you may ignore this alarm.

Front Panel Message

Input 1 Loss of input signal

Possible Cause(s)

- A cable is loose, disconnected, or defective.
- An upstream device providing input to the GQAM modulator failed or is offline.
- The GQAM modulator is defective.

Check and Correct

A cable is loose, disconnected, or defective

Check for loose cable connections or defective cables at the ASI inputs on the back panel of the GQAM modulator, connect any disconnected cables, then tighten any loose cable connections, and replace any defective cables.

Upstream device failed or offline

- 1 Verify that the ASI outputs of upstream devices are functioning correctly.
- 2 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 3 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 4 If the alarm continues to occur, contact Cisco Services for further assistance.

GQAM modulator is defective

- 1 Replace the GQAM modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the GQAM modulator.
- 2 Contact Cisco Services for further assistance.

GQAM Modulator Alarm ID 53 (35 Hex)

The **Input 1 MPEG Packets Error** alarm occurs when there are errors in the headers of the MPEG packets at the ASI In 1 port in the GQAM modulator. Errors include an invalid MPEG packet header where the first byte (for example, sync byte) is not equal to 47 Hex (0x47), or where the MPEG packet size is not exactly 188 bytes. There is a potential for loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the GQAM modulator that is sending this alarm.

This alarm may also occur when the ASI cable is disconnected and then clear before you reconnect the cable. This alarm clear occurs because the MPEG stream is disrupted and the device detects that the input signal is completely lost.

Note: This alarm is self-clearing and may be intermittent. Single instances of this alarm that clear automatically and that do not reappear are not a cause for concern.

Front Panel Message

Input 1 Errored MPEG packet

Possible Cause(s)

- A cable is loose, disconnected, or defective.
- There are data errors on the satellite link.
- The rate of change of the IEC exceeds the allowed threshold.
- Upstream devices that provide input to the GQAM modulator are sending errored MPEG packets.
- There is defective local MPEG coding.
- The GQAM modulator is defective.

Check and Correct

A cable is loose, disconnected, or defective

Check for loose connections or defective cables, tighten any loose cable connections, connect any disconnected cables, and replace any defective cables.

Note: This alarm may also occur when the ASI cable is disconnected and then clear before you reconnect the cable. This is normal.

Data errors on the satellite link

Contact your signal provider to verify if there are any problems with their satellite transmissions.

Chapter 3 GQAM Modulator Alarms

IEC exceeds threshold

Clean up the MPEG signal input to the GQAM modulator by checking the IRT, RTE, and MPEG encoder.

Upstream devices sending errored MPEG packets

- 1 Check the upstream devices that are sending MPEG packets to the ASI In 1 port on the GQAM modulator.
- 2 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 3 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 4 If the alarm continues to occur, contact Cisco Services for further assistance.

Defective local MPEG coding

Check the local source devices that are providing MPEG content to the GQAM modulator.

GQAM modulator is defective

- 1 Replace the GQAM modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the GQAM modulator.
- 2 Contact Cisco Services for further assistance.

GQAM Modulator Alarm ID 54 (36 Hex)

The **Input 1 FIFO Overflow Error** alarm occurs when there is a FIFO buffer overflow at the ASI In 1 port on the GQAM modulator, and packet data is lost. There is a potential for loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the GQAM modulator that is sending this alarm.

Note: This alarm is self-clearing and may be intermittent. Single instances of this alarm that clear automatically and that do not reappear are not a cause for concern.

Front Panel Message

Input 1 FIFO overflow

Possible Cause(s)

- The data rate as defined from the EC for the GQAM modulator sessions is too low, which also means that the data rate of the ASI input to the GQAM modulator is too high.
- There are too many sessions defined for the GQAM modulator from the EC.
- The modulation mode is incorrect.
- Upstream devices are sending too many MPEG packets to the GQAM modulator.
- A hardware problem occurred

Check and Correct

Data rate too low

- 1 Reduce the amount of incoming data.
- 2 Reduce the amount of data added to the stream.
- 3 Increase the GQAM modulation mode.
- 4 Verify and correct session rate targets and threshold values.

Too many sessions defined

Reduce the total number of MPEG programs by deleting sessions.

Modulation mode incorrect

Verify and correct the modulation mode.

Upstream devices sending too many MPEG packets

Check the upstream devices that are sending MPEG packets to the ASI input ports on the GQAM modulator.

Chapter 3 GQAM Modulator Alarms

Hardware problem

- 1 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 2 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 3 Replace the GQAM modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the GQAM modulator.
- 4 If the alarm continues to occur, contact Cisco Services for further assistance.

GQAM Modulator Alarm ID 55 (37 Hex)

The **Input 1 Excess Packets Dumped** alarm occurs when there is excessive bandwidth utilization on one or more channels at the ASI In 1 port on the GQAM modulator. Packets for those channels are being dumped so as not to affect the other channels.

There is potential loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the GQAM modulator that is sending this alarm.

Note: This alarm is self-clearing and may be intermittent. Single instances of this alarm that clear automatically and that do not reappear are not a cause for concern.

Front Panel Message

Input 1 Packets were dumped

Possible Cause(s)

- The data rate as defined from the EC for the GQAM modulator sessions is too low, which also means that the data rate of the ASI input to the GQAM modulator is too high.
- There are too many sessions defined for the GQAM modulator from the EC.
- The modulation mode is incorrect.
- Upstream devices are sending too many MPEG packets to the GQAM modulator.
- A hardware problem occurred.

Check and Correct

Data rate too low

- 1 Reduce the amount of incoming data.
- 2 Reduce the amount of data added to the stream.
- 3 Increase the GQAM modulation mode.
- 4 Verify and correct session rate targets and threshold values.

Too many sessions defined

Reduce the total number of MPEG programs by deleting sessions.

Modulation mode incorrect

Verify and correct the modulation mode.

Chapter 3 GQAM Modulator Alarms

Upstream devices sending too many MPEG packets

Check the upstream devices that are sending MPEG packets to the ASI input ports on the GQAM modulator.

Hardware problem

- 1 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 2 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 3 Replace the GQAM modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the GQAM modulator.
- 4 If the alarm continues to occur, contact Cisco Services for further assistance.

GQAM Modulator Alarm ID 56 (38 Hex)

The **Input 2 Loss of Signal Error** alarm occurs when there is no ASI signal to the ASI In 2 port in the GQAM modulator. Active program and data services that are present on ASI In 2 are not available.

Important! If you receive the loss of signal alarm an input that you are intentionally not using, you may ignore this alarm.

Front Panel Message

Input 2 Loss of input signal

Possible Cause(s)

- A cable is loose, disconnected, or defective.
- An upstream device providing input to the GQAM modulator failed or is offline.
- The GQAM modulator is defective.

Check and Correct

A cable is loose, disconnected, or defective

Check for loose cable connections or defective cables at the ASI inputs on the back panel of the GQAM modulator, connect any disconnected cables, then tighten any loose cable connections, and replace any defective cables.

Upstream device failed or offline

- 1 Verify that the ASI outputs of upstream devices are functioning correctly.
- 2 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 3 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 4 If the alarm continues to occur, contact Cisco Services for further assistance.

GQAM modulator is defective

- 1 Replace the GQAM modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the GQAM modulator.
- 2 Contact Cisco Services for further assistance.

GQAM Modulator Alarm ID 57 (39 Hex)

The **Input 2 MPEG Packets Error** alarm occurs when there are errors in the headers of the MPEG packets at the ASI In 2 port in the GQAM modulator. Errors include an invalid MPEG packet header where the first byte (for example, sync byte) is not equal to 47 Hex (0x47), or where the MPEG packet size is not exactly 188 bytes. There is a potential for loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the GQAM modulator that is sending this alarm.

This alarm may also occur when the ASI cable is disconnected and then clear before you reconnect the cable. This clear occurs because the MPEG stream is disrupted and the device detects that the input signal is completely lost.

Note: This alarm is self-clearing and may be intermittent. Single instances of this alarm that clear automatically and that do not reappear are not a cause for concern.

Front Panel Message

Input 2 Errored MPEG packet

Possible Cause(s)

- A cable is loose, disconnected, or defective.
- There are data errors on the satellite link.
- The rate of change of the IEC exceeds the allowed threshold.
- Upstream devices that provide input to the GQAM modulator are sending errored MPEG packets.
- There is defective local MPEG coding.
- The GQAM modulator is defective.

Check and Correct

A cable is loose, disconnected, or defective

Check for loose connections or defective cables, tighten any loose cable connections, connect any disconnected cables, and replace any defective cables.

Note: This alarm may also occur when the ASI cable is disconnected and then clear before you reconnect the cable. This is normal.

Data errors on the satellite link

Contact your signal provider to verify if there are any problems with their satellite transmissions.

IEC exceeds threshold

Clean up the MPEG signal input to the GQAM modulator by checking the IRT, RTE, and MPEG encoder.

Upstream devices sending errored MPEG packets

- 1 Check the upstream devices that are sending MPEG packets to the ASI In 2 port on the GQAM modulator.
- 2 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 3 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 4 If the alarm continues to occur, contact Cisco Services for further assistance.

Defective local MPEG coding

Check the local source devices that are providing MPEG content to the GQAM modulator.

GQAM modulator is defective

- 1 Replace the GQAM modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the GQAM modulator.
- 2 Contact Cisco Services for further assistance.

GQAM Modulator Alarm ID 58 (3A Hex)

The **Input 2 FIFO Overflow Error** alarm occurs when there is a FIFO buffer overflow at the ASI In 2 port on the GQAM modulator, and packet data is lost. There is a potential for loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the GQAM modulator that is sending this alarm.

Note: This alarm is self-clearing and may be intermittent. Single instances of this alarm that clear automatically and that do not reappear are not a cause for concern.

Front Panel Message

Input 2 FIFO overflow

Possible Cause(s)

- The data rate as defined from the EC for the GQAM modulator sessions is too low, which also means that the data rate of the ASI input to the GQAM modulator is too high.
- There are too many sessions defined for the GQAM modulator from the EC.
- The modulation mode is incorrect.
- Upstream devices are sending too many MPEG packets to the GQAM modulator.
- A hardware problem occurred.

Check and Correct

Data rate too low

- 1 Reduce the amount of incoming data.
- 2 Reduce the amount of data added to the stream.
- 3 Increase the GQAM modulation mode.
- 4 Verify and correct session rate targets and threshold values.

Too many sessions defined

Reduce the total number of MPEG programs by deleting sessions.

Modulation mode incorrect

Verify and correct the modulation mode.

Upstream devices sending too many MPEG packets

Check the upstream devices that are sending MPEG packets to the ASI input ports on the GQAM modulator.

Hardware problem

- 1** Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 2** Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 3** Replace the GQAM modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the GQAM modulator.
- 4** If the alarm continues to occur, contact Cisco Services for further assistance.

GQAM Modulator Alarm ID 59 (3B Hex)

The **Input 2 Excess Packets Dumped** alarm occurs when there is excessive bandwidth utilization on one or more channels at the ASI In 2 port on the GQAM modulator. Packets for those channels are being dumped so as not to affect the other channels.

There is potential loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the GQAM modulator that is sending this alarm.

Note: This alarm is self-clearing and may be intermittent. Single instances of this alarm that clear automatically and that do not reappear are not a cause for concern.

Front Panel Message

Input 2 Packets were dumped

Possible Cause(s)

- The data rate as defined from the EC for the GQAM modulator sessions is too low, which also means that the data rate of the ASI input to the GQAM modulator is too high.
- There are too many sessions defined for the GQAM modulator from the EC.
- The modulation mode is incorrect.
- Upstream devices are sending too many MPEG packets to the GQAM modulator.
- A hardware problem occurred.

Check and Correct

Data rate too low

- 1 Reduce the amount of incoming data.
- 2 Reduce the amount of data added to the stream.
- 3 Increase the GQAM modulation mode.
- 4 Verify and correct session rate targets and threshold values

Too many sessions defined

Reduce the total number of MPEG programs by deleting sessions.

Modulation mode incorrect

Verify and correct the modulation mode.

Upstream devices sending too many MPEG packets

Check the upstream devices that are sending MPEG packets to the ASI input ports on the GQAM modulator.

Hardware problem

- 1** Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 2** Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 3** Replace the GQAM modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the GQAM modulator.
- 4** If the alarm continues to occur, contact Cisco Services for further assistance.

GQAM Modulator Alarm ID 60 (3C Hex)

The **Input 3 Loss of Signal Error** alarm occurs when there is no ASI signal to the ASI In 3 port in the GQAM modulator. Active program and data services that are present on ASI In 3 are not available.

Important! If you receive the loss of signal alarm an input that you are intentionally not using, you may ignore this alarm.

Front Panel Message

Input 3 Loss of input signal

Possible Cause(s)

- A cable is loose, disconnected, or defective.
- An upstream device providing input to the GQAM modulator failed or is offline.
- The GQAM modulator is defective.

Check and Correct

A cable is loose, disconnected, or defective

Check for loose cable connections or defective cables at the ASI inputs on the back panel of the GQAM modulator, connect any disconnected cables, then tighten any loose cable connections, and replace any defective cables.

Upstream device failed or offline

- 1 Verify that the ASI outputs of upstream devices are functioning correctly.
- 2 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 3 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 4 If the alarm continues to occur, contact Cisco Services for further assistance.

GQAM modulator is defective

- 1 Replace the GQAM modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the GQAM modulator.
- 2 Contact Cisco Services for further assistance.

GQAM Modulator Alarm ID 61 (3D Hex)

The **Input 3 MPEG Packets Error** alarm occurs when there are errors in the headers of the MPEG packets at the ASI In 3 port in the GQAM modulator. Errors include an invalid MPEG packet header where the first byte (for example, sync byte) is not equal to 47 Hex (0x47), or where the MPEG packet size is not exactly 188 bytes. There is a potential for loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the GQAM modulator that is sending this alarm.

This alarm may also occur when the ASI cable is disconnected and then clear before you reconnect the cable. This clear occurs because the MPEG stream is disrupted and the device detects that the input signal is completely lost.

Note: This alarm is self-clearing and may be intermittent. Single instances of this alarm that clear automatically and that do not reappear are not a cause for concern.

Front Panel Message

Input 3 Errored MPEG packet

Possible Cause(s)

- A cable is loose, disconnected, or defective.
- There are data errors on the satellite link.
- The rate of change of the IEC exceeds the allowed threshold.
- Upstream devices that provide input to the GQAM modulator are sending errored MPEG packets.
- There is defective local MPEG coding.
- The GQAM modulator is defective.

Check and Correct

A cable is loose, disconnected, or defective

Check for loose connections or defective cables, tighten any loose cable connections, connect any disconnected cables, and replace any defective cables.

Note: This alarm may also occur when the ASI cable is disconnected and then clear before you reconnect the cable. This is normal.

Data errors on the satellite link

Contact your signal provider to verify if there are any problems with their satellite transmissions.

Chapter 3 GQAM Modulator Alarms

IEC exceeds threshold

Clean up the MPEG signal input to the GQAM modulator by checking the IRT, RTE, and MPEG encoder.

Upstream devices sending errored MPEG packets

- 1 Check the upstream devices that are sending MPEG packets to the ASI In 3 port on the GQAM modulator.
- 2 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 3 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 4 If the alarm continues to occur, contact Cisco Services for further assistance.

Defective local MPEG coding

Check the local source devices that are providing MPEG content to the GQAM modulator.

GQAM modulator is defective

- 1 Replace the GQAM modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the GQAM modulator.
- 2 Contact Cisco Services for further assistance.

GQAM Modulator Alarm ID 62 (3E Hex)

The **Input 3 FIFO Overflow Error** alarm occurs when there is a FIFO buffer overflow at the ASI In 3 port on the GQAM modulator, and packet data is lost. There is a potential for loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the GQAM modulator that is sending this alarm.

Note: This alarm is self-clearing and may be intermittent. Single instances of this alarm that clear automatically and that do not reappear are not a cause for concern.

Front Panel Message

Input 3 FIFO overflow

Possible Cause(s)

- The data rate as defined from the EC for the GQAM modulator sessions is too low, which also means that the data rate of the ASI input to the GQAM modulator is too high.
- There are too many sessions defined for the GQAM modulator from the EC.
- The modulation mode is incorrect.
- Upstream devices are sending too many MPEG packets to the GQAM modulator.
- A hardware problem occurred.

Check and Correct

Data rate too low

- 1 Reduce the amount of incoming data.
- 2 Reduce the amount of data added to the stream.
- 3 Increase the GQAM modulation mode.
- 4 Verify and correct session rate targets and threshold values.

Too many sessions defined

Reduce the total number of MPEG programs by deleting sessions.

Modulation mode incorrect

Verify and correct the modulation mode.

Upstream devices sending too many MPEG packets

Check the upstream devices that are sending MPEG packets to the ASI input ports on the GQAM modulator.

Chapter 3 GQAM Modulator Alarms

Hardware problem

- 1 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 2 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 3 Replace the GQAM modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the GQAM modulator.
- 4 If the alarm continues to occur, contact Cisco Services for further assistance.

GQAM Modulator Alarm ID 63 (3F Hex)

The **Input 3 Excess Packets Dumped** alarm occurs when there is excessive bandwidth utilization on one or more channels at the ASI In 3 port on the GQAM modulator. Packets for those channels are being dumped so as not to affect the other channels.

There is potential loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the GQAM modulator that is sending this alarm.

Note: This alarm is self-clearing and may be intermittent. Single instances of this alarm that clear automatically and that do not reappear are not a cause for concern.

Front Panel Message

Input 3 Packets were dumped

Possible Cause(s)

- The data rate as defined from the EC for the GQAM modulator sessions is too low, which also means that the data rate of the ASI input to the GQAM modulator is too high.
- There are too many sessions defined for the GQAM modulator from the EC.
- The modulation mode is incorrect.
- Upstream devices are sending too many MPEG packets to the GQAM modulator.
- A hardware problem occurred.

Check and Correct

Data rate too low

- 1 Reduce the amount of incoming data.
- 2 Reduce the amount of data added to the stream.
- 3 Increase the GQAM modulation mode.
- 4 Verify and correct session rate targets and threshold values.

Too many sessions defined

Reduce the total number of MPEG programs by deleting sessions.

Modulation mode incorrect

Verify and correct the modulation mode.

Chapter 3 GQAM Modulator Alarms

Upstream devices sending too many MPEG packets

Check the upstream devices that are sending MPEG packets to the ASI input ports on the GQAM modulator.

Hardware problem

- 1 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 2 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 3 Replace the GQAM modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the GQAM modulator.
- 4 If the alarm continues to occur, contact Cisco Services for further assistance.

GQAM Modulator Alarm ID 64 (40 Hex)

The **Input 4 Loss of Signal Error** alarm occurs when there is no ASI signal to the ASI In 4 port in the GQAM modulator. Active program and data services that are present on ASI In 4 are not available.

Important! If you receive the loss of signal alarm an input that you are intentionally not using, you may ignore this alarm.

Front Panel Message

Input 4 Loss of input signal

Possible Cause(s)

- A cable is loose, disconnected, or defective.
- An upstream device providing input to the GQAM modulator failed or is offline.
- The GQAM modulator is defective.

Check and Correct

A cable is loose, disconnected, or defective

Check for loose cable connections or defective cables at the ASI inputs on the back panel of the GQAM modulator, connect any disconnected cables, then tighten any loose cable connections, and replace any defective cables.

Upstream device failed or offline

- 1 Verify that the ASI outputs of upstream devices are functioning correctly.
- 2 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 3 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 4 If the alarm continues to occur, contact Cisco Services for further assistance.

GQAM modulator is defective

- 1 Replace the GQAM modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the GQAM modulator.
- 2 Contact Cisco Services for further assistance.

GQAM Modulator Alarm ID 65 (41 Hex)

The **Input 4 MPEG Packets Error** alarm occurs when there are errors in the headers of the MPEG packets at the ASI In 4 port in the GQAM modulator. Errors include an invalid MPEG packet header where the first byte (for example, sync byte) is not equal to 47 Hex (0x47), or where the MPEG packet size is not exactly 188 bytes. There is a potential for loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the GQAM modulator that is sending this alarm.

This alarm may also occur when the ASI cable is disconnected and then clear before you reconnect the cable. This clear occurs because the MPEG stream is disrupted and the device detects that the input signal is completely lost.

Note: This alarm is self-clearing and may be intermittent. Single instances of this alarm that clear automatically and that do not reappear are not a cause for concern.

Front Panel Message

Input 4 Errored MPEG packet

Possible Cause(s)

- A cable is loose, disconnected, or defective.
- There are data errors on the satellite link.
- The rate of change of the IEC exceeds the allowed threshold.
- Upstream devices that provide input to the GQAM modulator are sending errored MPEG packets.
- There is defective local MPEG coding.
- The GQAM modulator is defective.

Check and Correct

A cable is loose, disconnected, or defective

Check for loose connections or defective cables, tighten any loose cable connections, connect any disconnected cables, and replace any defective cables.

Note: This alarm may also occur when the ASI cable is disconnected and then clear before you reconnect the cable. This is normal.

Data errors on the satellite link

Contact your signal provider to verify if there are any problems with their satellite transmissions.

IEC exceeds threshold

Clean up the MPEG signal input to the GQAM modulator by checking the IRT, RTE, and MPEG encoder.

Upstream devices sending errored MPEG packets

- 1 Check the upstream devices that are sending MPEG packets to the ASI In 4 port on the GQAM modulator.
- 2 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 3 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 4 If the alarm continues to occur, contact Cisco Services for further assistance.

Defective local MPEG coding

Check the local source devices that are providing MPEG content to the GQAM modulator.

GQAM modulator is defective

- 1 Replace the GQAM modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the GQAM modulator.
- 2 Contact Cisco Services for further assistance.

GQAM Modulator Alarm ID 66 (42 Hex)

The **Input 4 FIFO Overflow Error** alarm occurs when there is a FIFO buffer overflow at the ASI In 4 port on the GQAM modulator, and packet data is lost. There is a potential for loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the GQAM modulator that is sending this alarm.

Note: This alarm is self-clearing and may be intermittent. Single instances of this alarm that clear automatically and that do not reappear are not a cause for concern.

Front Panel Message

Input 4 FIFO overflow

Possible Cause(s)

- The data rate as defined from the EC for the GQAM modulator sessions is too low, which also means that the data rate of the ASI input to the GQAM modulator is too high.
- There are too many sessions defined for the GQAM modulator from the EC.
- The modulation mode is incorrect.
- Upstream devices are sending too many MPEG packets to the GQAM modulator.
- A hardware problem occurred.

Check and Correct

Data rate too low

- 1 Reduce the amount of incoming data.
- 2 Reduce the amount of data added to the stream.
- 3 Increase the GQAM modulation mode.
- 4 Verify and correct session rate targets and threshold values.

Too many sessions defined

Reduce the total number of MPEG programs by deleting sessions.

Modulation mode incorrect

Verify and correct the modulation mode.

Upstream devices sending too many MPEG packets

Check the upstream devices that are sending MPEG packets to the ASI input ports on the GQAM modulator.

Hardware problem

- 1** Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 2** Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 3** Replace the GQAM modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the GQAM modulator.
- 4** If the alarm continues to occur, contact Cisco Services for further assistance.

GQAM Modulator Alarm ID 67 (43 Hex)

The **Input 4 Excess Packets Dumped** alarm occurs when there is excessive bandwidth utilization on one or more channels at the ASI In 4 port on the GQAM modulator. Packets for those channels are being dumped so as not to affect the other channels.

There is potential loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the GQAM modulator that is sending this alarm.

Note: This alarm is self-clearing and may be intermittent. Single instances of this alarm that clear automatically and that do not reappear are not a cause for concern.

Front Panel Message

Input 4 Packets were dumped

Possible Cause(s)

- The data rate as defined from the EC for the GQAM modulator sessions is too low, which also means that the data rate of the ASI input to the GQAM modulator is too high.
- There are too many sessions defined for the GQAM modulator from the EC.
- The modulation mode is incorrect.
- Upstream devices are sending too many MPEG packets to the GQAM modulator.
- A hardware problem occurred.

Check and Correct

Data rate too low

- 1 Reduce the amount of incoming data.
- 2 Reduce the amount of data added to the stream.
- 3 Increase the GQAM modulation mode.
- 4 Verify and correct session rate targets and threshold values.

Too many sessions defined

Reduce the total number of MPEG programs by deleting sessions.

Modulation mode incorrect

Verify and correct the modulation mode.

Upstream devices sending too many MPEG packets

Check the upstream devices that are sending MPEG packets to the ASI input ports on the GQAM modulator.

Hardware problem

- 1** Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 2** Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 3** Replace the GQAM modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the GQAM modulator.
- 4** If the alarm continues to occur, contact Cisco Services for further assistance.

GQAM Modulator Alarm ID 68 (44 Hex)

The **Input 5 Loss of Signal Error** alarm occurs when there is no input signal to the GbE port in the GQAM modulator. Active program and data services that are present on the GbE port are not available.

Important! If you receive the loss of signal alarm on an input that you are intentionally not using, you may ignore this alarm.

Front Panel Message

Input 5 Loss of input signal

Possible Cause(s)

- A cable is loose, disconnected, or defective.
- An upstream device providing input to the GQAM modulator failed or is offline.
- The GQAM modulator is defective.

Check and Correct

A cable is loose, disconnected, or defective

Check for loose cable connections or defective cables at the GbE input port on the back panel of the GQAM modulator, connect any disconnected cables, then tighten any loose cable connections, and replace any defective cables.

Upstream device failed or offline

- 1 Verify that the outputs of upstream devices sending data to the GbE port are functioning correctly.
- 2 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 3 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 4 If the alarm continues to occur, contact Cisco Services for further assistance.

GQAM modulator is defective

- 1 Replace the GQAM modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the GQAM modulator.
- 2 Contact Cisco Services for further assistance.

GQAM Modulator Alarm ID 69 (45 Hex)

The **Input 5 MPEG Packets Error** alarm occurs when there are errors in the headers of the MPEG packets at the GbE port in the GQAM modulator. Errors include an invalid MPEG packet header where the first byte (for example, sync byte) is not equal to 47 Hex (0x47), or where the MPEG packet size is not exactly 188 bytes. There is a potential for loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the GQAM modulator that is sending this alarm.

This alarm may also occur when the input cable is disconnected and then clear before you reconnect the cable. This clear occurs because the MPEG stream is disrupted and the device detects that the input signal is completely lost.

Note: This alarm is self-clearing and may be intermittent. Single instances of this alarm that clear automatically and that do not reappear are not a cause for concern.

Front Panel Message

Input 5 Errored MPEG packet

Possible Cause(s)

- A cable is loose, disconnected, or defective.
- There are data errors on the satellite link.
- The rate of change of the IEC exceeds the allowed threshold.
- Upstream devices that provide input to the GQAM modulator are sending errored MPEG packets.
- There is defective local MPEG coding.
- The GQAM modulator is defective.

Check and Correct

A cable is loose, disconnected, or defective

Check for loose connections or defective cables, tighten any loose cable connections, connect any disconnected cables, and replace any defective cables.

Note: This alarm may also occur when the input cable is disconnected and then clear before you reconnect the cable. This is normal.

Data errors on the satellite link

Contact your signal provider to verify if there are any problems with their satellite transmissions.

Chapter 3 GQAM Modulator Alarms

IEC exceeds threshold

Clean up the MPEG signal input to the GQAM modulator by checking the IRT, RTE, and MPEG encoder.

Upstream devices sending errored MPEG packets

- 1 Check the upstream devices that are sending MPEG packets to the GbE port on the GQAM modulator.
- 2 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 3 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 4 If the alarm continues to occur, contact Cisco Services for further assistance.

Defective local MPEG coding

Check the local source devices that are providing MPEG content to the GQAM modulator.

GQAM modulator is defective

- 1 Replace the GQAM modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the GQAM modulator.
- 2 Contact Cisco Services for further assistance.

GQAM Modulator Alarm ID 70 (46 Hex)

The **Input 5 FIFO Overflow Error** alarm occurs when there is a FIFO buffer overflow at the GbE port on the GQAM modulator, and packet data is lost. There is a potential for loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the GQAM modulator that is sending this alarm.

Note: This alarm is self-clearing and may be intermittent. Single instances of this alarm that clear automatically and that do not reappear are not a cause for concern.

Front Panel Message

Input 5 FIFO overflow

Possible Cause(s)

- The data rate as defined from the EC for the GQAM modulator sessions is too low, which also means that the data rate of the GbE input to the GQAM modulator is too high.
- There are too many sessions defined for the GQAM modulator from the EC.
- The modulation mode is incorrect.
- Upstream devices are sending too many MPEG packets to the GQAM modulator.
- A hardware problem occurred.

Check and Correct

Data rate too low

- 1 Reduce the amount of incoming data.
- 2 Reduce the amount of data added to the stream.
- 3 Increase the GQAM modulation mode.
- 4 Verify and correct session rate targets and threshold values.

Too many sessions defined

Reduce the total number of MPEG programs by deleting sessions.

Modulation mode incorrect

Verify and correct the modulation mode.

Upstream devices sending too many MPEG packets

Check the upstream devices that are sending MPEG packets to GbE port on the GQAM modulator.

Chapter 3 GQAM Modulator Alarms

Hardware problem

- 1 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 2 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 3 Replace the GQAM modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the GQAM modulator.
- 4 If the alarm continues to occur, contact Cisco Services for further assistance.

GQAM Modulator Alarm ID 71 (47 Hex)

The **Input 5 Excess Packets Dumped** alarm occurs when there is excessive bandwidth utilization on one or more channels at the GbE port on the GQAM modulator. Packets for those channels are being dumped so as not to affect the other channels.

There is potential loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the GQAM modulator that is sending this alarm.

Note: This alarm is self-clearing and may be intermittent. Single instances of this alarm that clear automatically and that do not reappear are not a cause for concern.

Front Panel Message

Input 5 Packets were dumped

Possible Cause(s)

- The data rate as defined from the EC for the GQAM modulator sessions is too low, which also means that the data rate of the ASI input to the GQAM modulator is too high.
- There are too many sessions defined for the GQAM modulator from the EC.
- The modulation mode is incorrect.
- Upstream devices are sending too many MPEG packets to the GQAM modulator.
- A hardware problem occurred.

Check and Correct

Data rate too low

- 1 Reduce the amount of incoming data.
- 2 Reduce the amount of data added to the stream.
- 3 Increase the GQAM modulation mode.
- 4 Verify and correct session rate targets and threshold values.

Too many sessions defined

Reduce the total number of MPEG programs by deleting sessions.

Modulation mode incorrect

Verify and correct the modulation mode.

Chapter 3 GQAM Modulator Alarms

Upstream devices sending too many MPEG packets

Check the upstream devices that are sending MPEG packets to the ASI input ports on the GQAM modulator.

Hardware problem

- 1 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 2 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 3 Replace the GQAM modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the GQAM modulator.
- 4 If the alarm continues to occur, contact Cisco Services for further assistance.

GQAM Modulator Alarm ID 72 (48 Hex)

The **Output 1 Packets Dropped** alarm occurs when the GQAM modulator is dropping low priority packets at output channel 1. Low priority packets are being dropped because the number of packets at output Channel 1 exceeds its capacity.

Note: This alarm is self-clearing and may be intermittent. Single instances of this alarm that clear automatically and that do not reappear are not a cause for concern.

There is a low potential for loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the GQAM modulator that is sending this alarm.

Front Panel Message

OUT1 Packets dropped

Possible Cause(s)

- The data rate as defined from the EC for the GQAM modulator sessions is too low, which also means that the data rate of the ASI input to the GQAM modulator is too high.
- There are too many sessions defined for the GQAM modulator from the EC.
- The modulation mode is incorrect.
- A hardware problem occurred.

Check and Correct

Data rate is too low

- 1 Reduce the amount of incoming data.
- 2 Reduce the amount of data added to the stream.
- 3 Increase the GQAM modulation mode.
- 4 Verify and correct session rate targets and threshold values.

Too many sessions defined

Reduce the total number of MPEG programs by deleting sessions.

Modulation mode is incorrect

Verify and correct the modulation mode.

Chapter 3 GQAM Modulator Alarms

Hardware problem

- 1 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 2 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 3 Replace the GQAM modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the GQAM modulator.
- 4 If the alarm continues to occur, contact Cisco Services for further assistance.

GQAM Modulator Alarm ID 73 (49 Hex)

The **Output 2 Packets Dropped** alarm occurs when the GQAM modulator is dropping low priority packets at output channel 2. Low priority packets are being dropped because the number of packets at output channel 2 exceeds its capacity.

Note: This alarm is self-clearing and may be intermittent. Single instances of this alarm that clear automatically and that do not reappear are not a cause for concern.

There is a low potential for loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the GQAM modulator that is sending this alarm.

Front Panel Message

OUT2 Packets dropped

Possible Cause(s)

- The data rate as defined from the EC for the GQAM modulator sessions is too low, which also means that the data rate of the ASI input to the GQAM modulator is too high.
- There are too many sessions defined for the GQAM modulator from the EC.
- The modulation mode is incorrect.
- A hardware problem occurred.

Check and Correct

Data rate is too low

- 1 Reduce the amount of incoming data.
- 2 Reduce the amount of data added to the stream.
- 3 Increase the GQAM modulation mode.
- 4 Verify and correct session rate targets and threshold values.

Too many sessions defined

Reduce the total number of MPEG programs by deleting sessions.

Modulation mode is incorrect

Verify and correct the modulation mode.

Chapter 3 GQAM Modulator Alarms

Hardware problem

- 1 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 2 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 3 Replace the GQAM modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the GQAM modulator.
- 4 If the alarm continues to occur, contact Cisco Services for further assistance.

GQAM Modulator Alarm ID 74 (4A Hex)

The **Output 3 Packets Dropped** alarm occurs when the GQAM modulator is dropping low priority packets at output channel 3. Low priority packets are being dropped because the number of packets at output channel 3 exceeds its capacity.

Note: This alarm is self-clearing and may be intermittent. Single instances of this alarm that clear automatically and that do not reappear are not a cause for concern.

There is a low potential for loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the GQAM modulator that is sending this alarm.

Front Panel Message

OUT3 Packets dropped

Possible Cause(s)

- The data rate as defined from the EC for the GQAM modulator sessions is too low, which also means that the data rate of the ASI input to the GQAM modulator is too high.
- There are too many sessions defined for the GQAM modulator from the EC.
- The modulation mode is incorrect.
- A hardware problem occurred.

Check and Correct

Data rate is too low

- 1 Reduce the amount of incoming data.
- 2 Reduce the amount of data added to the stream.
- 3 Increase the GQAM modulation mode.
- 4 Verify and correct session rate targets and threshold values.

Too many sessions defined

Reduce the total number of MPEG programs by deleting sessions.

Modulation mode is incorrect

Verify and correct the modulation mode.

Chapter 3 GQAM Modulator Alarms

Hardware problem

- 1 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 2 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 3 Replace the GQAM modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the GQAM modulator.
- 4 If the alarm continues to occur, contact Cisco Services for further assistance.

GQAM Modulator Alarm ID 75 (4B Hex)

The **Output 4 Packets Dropped** alarm occurs when the GQAM modulator is dropping low priority packets at output channel 4. Low priority packets are being dropped because the number of packets at output channel 4 exceeds its capacity.

Note: This alarm is self-clearing and may be intermittent. Single instances of this alarm that clear automatically and that do not reappear are not a cause for concern.

There is a low potential for loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the GQAM modulator that is sending this alarm.

Front Panel Message

OUT4 Packets dropped

Possible Cause(s)

- The data rate as defined from the EC for the GQAM modulator sessions is too low, which also means that the data rate of the ASI input to the GQAM modulator is too high.
- There are too many sessions defined for the GQAM modulator from the EC.
- The modulation mode is incorrect.
- A hardware problem occurred.

Check and Correct

Data rate is too low

- 1 Reduce the amount of incoming data.
- 2 Reduce the amount of data added to the stream.
- 3 Increase the GQAM modulation mode.
- 4 Verify and correct session rate targets and threshold values.

Too many sessions defined

Reduce the total number of MPEG programs by deleting sessions.

Modulation mode is incorrect

Verify and correct the modulation mode.

Chapter 3 GQAM Modulator Alarms

Hardware problem

- 1 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 2 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 3 Replace the GQAM modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the GQAM modulator.
- 4 If the alarm continues to occur, contact Cisco Services for further assistance.

GQAM Modulator Alarm ID 76 (4C Hex)

The **Output 5 Packets Dropped** alarm occurs when the GQAM modulator is dropping low priority packets at output channel 5. Low priority packets are being dropped because the number of packets at output channel 5 exceeds its capacity.

Note: This alarm is self-clearing and may be intermittent. Single instances of this alarm that clear automatically and that do not reappear are not a cause for concern.

There is a low potential for loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the GQAM modulator that is sending this alarm.

Front Panel Message

OUT5 Packets dropped

Possible Cause(s)

- The data rate as defined from the EC for the GQAM modulator sessions is too low, which also means that the data rate of the ASI input to the GQAM modulator is too high.
- There are too many sessions defined for the GQAM modulator from the EC.
- The modulation mode is incorrect.
- A hardware problem occurred.

Check and Correct

Data rate is too low

- 1 Reduce the amount of incoming data.
- 2 Reduce the amount of data added to the stream.
- 3 Increase the GQAM modulation mode.
- 4 Verify and correct session rate targets and threshold values.

Too many sessions defined

Reduce the total number of MPEG programs by deleting sessions.

Modulation mode is incorrect

Verify and correct the modulation mode.

Chapter 3 GQAM Modulator Alarms

Hardware problem

- 1 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 2 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 3 Replace the GQAM modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the GQAM modulator.
- 4 If the alarm continues to occur, contact Cisco Services for further assistance.

GQAM Modulator Alarm ID 77 (4D Hex)

The **Output 6 Packets Dropped** alarm occurs when the GQAM modulator is dropping low priority packets at output channel 6. Low priority packets are being dropped because the number of packets at output channel 6 exceeds its capacity.

Note: This alarm is self-clearing and may be intermittent. Single instances of this alarm that clear automatically and that do not reappear are not a cause for concern.

There is a low potential for loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the GQAM modulator that is sending this alarm.

Front Panel Message

OUT6 Packets dropped

Possible Cause(s)

- The data rate as defined from the EC for the GQAM modulator sessions is too low, which also means that the data rate of the ASI input to the GQAM modulator is too high.
- There are too many sessions defined for the GQAM modulator from the EC.
- The modulation mode is incorrect.
- A hardware problem occurred.

Check and Correct

Data rate is too low

- 1 Reduce the amount of incoming data.
- 2 Reduce the amount of data added to the stream.
- 3 Increase the GQAM modulation mode.
- 4 Verify and correct session rate targets and threshold values.

Too many sessions defined

Reduce the total number of MPEG programs by deleting sessions.

Modulation mode is incorrect

Verify and correct the modulation mode.

Chapter 3 GQAM Modulator Alarms

Hardware problem

- 1 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 2 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 3 Replace the GQAM modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the GQAM modulator.
- 4 If the alarm continues to occur, contact Cisco Services for further assistance.

GQAM Modulator Alarm ID 78 (4E Hex)

The **Output 7 Packets Dropped** alarm occurs when the GQAM modulator is dropping low priority packets at output channel 7. Low priority packets are being dropped because the number of packets at output channel 7 exceeds its capacity.

Note: This alarm is self-clearing and may be intermittent. Single instances of this alarm that clear automatically and that do not reappear are not a cause for concern.

There is a low potential for loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the GQAM modulator that is sending this alarm.

Front Panel Message

OUT7 Packets dropped

Possible Cause(s)

- The data rate as defined from the EC for the GQAM modulator sessions is too low, which also means that the data rate of the ASI input to the GQAM modulator is too high.
- There are too many sessions defined for the GQAM modulator from the EC.
- The modulation mode is incorrect.
- A hardware problem occurred.

Check and Correct

Data rate is too low

- 1 Reduce the amount of incoming data.
- 2 Reduce the amount of data added to the stream.
- 3 Increase the GQAM modulation mode.
- 4 Verify and correct session rate targets and threshold values.

Too many sessions defined

Reduce the total number of MPEG programs by deleting sessions.

Modulation mode is incorrect

Verify and correct the modulation mode.

Chapter 3 GQAM Modulator Alarms

Hardware problem

- 1 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 2 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 3 Replace the GQAM modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the GQAM modulator.
- 4 If the alarm continues to occur, contact Cisco Services for further assistance.

GQAM Modulator Alarm ID 79 (4F Hex)

The **Output 8 Packets Dropped** alarm occurs when the GQAM modulator is dropping low priority packets at output channel 8. Low priority packets are being dropped because the number of packets at output channel 8 exceeds its capacity.

Note: This alarm is self-clearing and may be intermittent. Single instances of this alarm that clear automatically and that do not reappear are not a cause for concern.

There is a low potential for loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the GQAM modulator that is sending this alarm.

Front Panel Message

OUT8 Packets dropped

Possible Cause(s)

- The data rate as defined from the EC for the GQAM modulator sessions is too low, which also means that the data rate of the ASI input to the GQAM modulator is too high.
- There are too many sessions defined for the GQAM modulator from the EC.
- The modulation mode is incorrect.
- A hardware problem occurred.

Check and Correct

Data rate is too low

- 1 Reduce the amount of incoming data.
- 2 Reduce the amount of data added to the stream.
- 3 Increase the GQAM modulation mode.
- 4 Verify and correct session rate targets and threshold values.

Too many sessions defined

Reduce the total number of MPEG programs by deleting sessions.

Modulation mode is incorrect

Verify and correct the modulation mode.

Chapter 3 GQAM Modulator Alarms

Hardware problem

- 1 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 2 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 3 Replace the GQAM modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the GQAM modulator.
- 4 If the alarm continues to occur, contact Cisco Services for further assistance.

GQAM Modulator Alarm ID 80 (50 Hex)

The **Output 9 Packets Dropped** alarm occurs when the GQAM modulator is dropping low priority packets at output channel 9. Low priority packets are being dropped because the number of packets at output channel 9 exceeds its capacity.

Note: This alarm is self-clearing and may be intermittent. Single instances of this alarm that clear automatically and that do not reappear are not a cause for concern.

There is a low potential for loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the GQAM modulator that is sending this alarm.

Front Panel Message

OUT9 Packets dropped

Possible Cause(s)

- The data rate as defined from the EC for the GQAM modulator sessions is too low, which also means that the data rate of the ASI input to the GQAM modulator is too high.
- There are too many sessions defined for the GQAM modulator from the EC.
- The modulation mode is incorrect.
- A hardware problem occurred.

Check and Correct

Data rate is too low

- 1 Reduce the amount of incoming data.
- 2 Reduce the amount of data added to the stream.
- 3 Increase the GQAM modulation mode.
- 4 Verify and correct session rate targets and threshold values.

Too many sessions defined

Reduce the total number of MPEG programs by deleting sessions.

Modulation mode is incorrect

Verify and correct the modulation mode.

Chapter 3 GQAM Modulator Alarms

Hardware problem

- 1 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 2 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 3 Replace the GQAM modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the GQAM modulator.
- 4 If the alarm continues to occur, contact Cisco Services for further assistance.

GQAM Modulator Alarm ID 81 (51 Hex)

The **Output 10 Packets Dropped** alarm occurs when the GQAM modulator is dropping low priority packets at output channel 10. Low priority packets are being dropped because the number of packets at output channel 10 exceeds its capacity.

Note: This alarm is self-clearing and may be intermittent. Single instances of this alarm that clear automatically and that do not reappear are not a cause for concern.

There is a low potential for loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the GQAM modulator that is sending this alarm.

Front Panel Message

OUT10 Packets dropped

Possible Cause(s)

- The data rate as defined from the EC for the GQAM modulator sessions is too low, which also means that the data rate of the ASI input to the GQAM modulator is too high.
- There are too many sessions defined for the GQAM modulator from the EC.
- The modulation mode is incorrect.
- A hardware problem occurred.

Check and Correct

Data rate is too low

- 1 Reduce the amount of incoming data.
- 2 Reduce the amount of data added to the stream.
- 3 Increase the GQAM modulation mode.
- 4 Verify and correct session rate targets and threshold values.

Too many sessions defined

Reduce the total number of MPEG programs by deleting sessions.

Modulation mode is incorrect

Verify and correct the modulation mode.

Chapter 3 GQAM Modulator Alarms

Hardware problem

- 1 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 2 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 3 Replace the GQAM modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the GQAM modulator.
- 4 If the alarm continues to occur, contact Cisco Services for further assistance.

GQAM Modulator Alarm ID 82 (52 Hex)

The **Output 11 Packets Dropped** alarm occurs when the GQAM modulator is dropping low priority packets at output channel 11. Low priority packets are being dropped because the number of packets at output channel 11 exceeds its capacity.

Note: This alarm is self-clearing and may be intermittent. Single instances of this alarm that clear automatically and that do not reappear are not a cause for concern.

There is a low potential for loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the GQAM modulator that is sending this alarm.

Front Panel Message

OUT11 Packets dropped

Possible Cause(s)

- The data rate as defined from the EC for the GQAM modulator sessions is too low, which also means that the data rate of the ASI input to the GQAM modulator is too high.
- There are too many sessions defined for the GQAM modulator from the EC.
- The modulation mode is incorrect.
- A hardware problem occurred.

Check and Correct

Data rate is too low

- 1 Reduce the amount of incoming data.
- 2 Reduce the amount of data added to the stream.
- 3 Increase the GQAM modulation mode.
- 4 Verify and correct session rate targets and threshold values.

Too many sessions defined

Reduce the total number of MPEG programs by deleting sessions.

Modulation mode is incorrect

Verify and correct the modulation mode.

Chapter 3 GQAM Modulator Alarms

Hardware problem

- 1 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 2 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 3 Replace the GQAM modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the GQAM modulator.
- 4 If the alarm continues to occur, contact Cisco Services for further assistance.

GQAM Modulator Alarm ID 83 (53 Hex)

The **Output 12 Packets Dropped** alarm occurs when the GQAM modulator is dropping low priority packets at output channel 12. Low priority packets are being dropped because the number of packets at output channel 12 exceeds its capacity.

Note: This alarm is self-clearing and may be intermittent. Single instances of this alarm that clear automatically and that do not reappear are not a cause for concern.

There is a low potential for loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the GQAM modulator that is sending this alarm.

Front Panel Message

OUT12 Packets dropped

Possible Cause(s)

- The data rate as defined from the EC for the GQAM modulator sessions is too low, which also means that the data rate of the ASI input to the GQAM modulator is too high.
- There are too many sessions defined for the GQAM modulator from the EC.
- The modulation mode is incorrect.
- A hardware problem occurred.

Check and Correct

Data rate is too low

- 1 Reduce the amount of incoming data.
- 2 Reduce the amount of data added to the stream.
- 3 Increase the GQAM modulation mode.
- 4 Verify and correct session rate targets and threshold values.

Too many sessions defined

Reduce the total number of MPEG programs by deleting sessions.

Modulation mode is incorrect

Verify and correct the modulation mode.

Chapter 3 GQAM Modulator Alarms

Hardware problem

- 1 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 2 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 3 Replace the GQAM modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the GQAM modulator.
- 4 If the alarm continues to occur, contact Cisco Services for further assistance.

GQAM Modulator Alarm ID 84 (54 Hex)

The **Output 13 Packets Dropped** alarm occurs when the GQAM modulator is dropping low priority packets at output channel 13. Low priority packets are being dropped because the number of packets at output channel 13 exceeds its capacity.

Note: This alarm is self-clearing and may be intermittent. Single instances of this alarm that clear automatically and that do not reappear are not a cause for concern.

There is a low potential for loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the GQAM modulator that is sending this alarm.

Front Panel Message

OUT13 Packets dropped

Possible Cause(s)

- The data rate as defined from the EC for the GQAM modulator sessions is too low, which also means that the data rate of the ASI input to the GQAM modulator is too high.
- There are too many sessions defined for the GQAM modulator from the EC.
- The modulation mode is incorrect.
- A hardware problem occurred.

Check and Correct

Data rate is too low

- 1 Reduce the amount of incoming data.
- 2 Reduce the amount of data added to the stream.
- 3 Increase the GQAM modulation mode.
- 4 Verify and correct session rate targets and threshold values.

Too many sessions defined

Reduce the total number of MPEG programs by deleting sessions.

Modulation mode is incorrect

Verify and correct the modulation mode.

Chapter 3 GQAM Modulator Alarms

Hardware problem

- 1 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 2 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 3 Replace the GQAM modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the GQAM modulator.
- 4 If the alarm continues to occur, contact Cisco Services for further assistance.

GQAM Modulator Alarm ID 85 (55 Hex)

The **Output 14 Packets Dropped** alarm occurs when the GQAM modulator is dropping low priority packets at output channel 14. Low priority packets are being dropped because the number of packets at output channel 14 exceeds its capacity.

Note: This alarm is self-clearing and may be intermittent. Single instances of this alarm that clear automatically and that do not reappear are not a cause for concern.

There is a low potential for loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the GQAM modulator that is sending this alarm.

Front Panel Message

OUT14 Packets dropped

Possible Cause(s)

- The data rate as defined from the EC for the GQAM modulator sessions is too low, which also means that the data rate of the ASI input to the GQAM modulator is too high.
- There are too many sessions defined for the GQAM modulator from the EC.
- The modulation mode is incorrect.
- A hardware problem occurred.

Check and Correct

Data rate is too low

- 1 Reduce the amount of incoming data.
- 2 Reduce the amount of data added to the stream.
- 3 Increase the GQAM modulation mode.
- 4 Verify and correct session rate targets and threshold values.

Too many sessions defined

Reduce the total number of MPEG programs by deleting sessions.

Modulation mode is incorrect

Verify and correct the modulation mode.

Chapter 3 GQAM Modulator Alarms

Hardware problem

- 1 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 2 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 3 Replace the GQAM modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the GQAM modulator.
- 4 If the alarm continues to occur, contact Cisco Services for further assistance.

GQAM Modulator Alarm ID 86 (56 Hex)

The **Output 15 Packets Dropped** alarm occurs when the GQAM modulator is dropping low priority packets at output channel 15. Low priority packets are being dropped because the number of packets at output channel 15 exceeds its capacity.

Note: This alarm is self-clearing and may be intermittent. Single instances of this alarm that clear automatically and that do not reappear are not a cause for concern.

There is a low potential for loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the GQAM modulator that is sending this alarm.

Front Panel Message

OUT15 Packets dropped

Possible Cause(s)

- The data rate as defined from the EC for the GQAM modulator sessions is too low, which also means that the data rate of the ASI input to the GQAM modulator is too high.
- There are too many sessions defined for the GQAM modulator from the EC.
- The modulation mode is incorrect.
- A hardware problem occurred.

Check and Correct

Data rate is too low

- 1 Reduce the amount of incoming data.
- 2 Reduce the amount of data added to the stream.
- 3 Increase the GQAM modulation mode.
- 4 Verify and correct session rate targets and threshold values.

Too many sessions defined

Reduce the total number of MPEG programs by deleting sessions.

Modulation mode is incorrect

Verify and correct the modulation mode.

Chapter 3 GQAM Modulator Alarms

Hardware problem

- 1 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 2 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 3 Replace the GQAM modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the GQAM modulator.
- 4 If the alarm continues to occur, contact Cisco Services for further assistance.

GQAM Modulator Alarm ID 87 (57 Hex)

The **Output 16 Packets Dropped** alarm occurs when the GQAM modulator is dropping low priority packets at output channel 16. Low priority packets are being dropped because the number of packets at output channel 16 exceeds its capacity.

Note: This alarm is self-clearing and may be intermittent. Single instances of this alarm that clear automatically and that do not reappear are not a cause for concern.

There is a low potential for loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the GQAM modulator that is sending this alarm.

Front Panel Message

OUT16 Packets dropped

Possible Cause(s)

- The data rate as defined from the EC for the GQAM modulator sessions is too low, which also means that the data rate of the ASI input to the GQAM modulator is too high.
- There are too many sessions defined for the GQAM modulator from the EC.
- The modulation mode is incorrect.
- A hardware problem occurred.

Check and Correct

Data rate is too low

- 1 Reduce the amount of incoming data.
- 2 Reduce the amount of data added to the stream.
- 3 Increase the GQAM modulation mode.
- 4 Verify and correct session rate targets and threshold values.

Too many sessions defined

Reduce the total number of MPEG programs by deleting sessions.

Modulation mode is incorrect

Verify and correct the modulation mode.

Chapter 3 GQAM Modulator Alarms

Hardware problem

- 1 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 2 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 3 Replace the GQAM modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the GQAM modulator.
- 4 If the alarm continues to occur, contact Cisco Services for further assistance.

GQAM Modulator Alarm ID 88 (58 Hex)

The **Hardware Failure** alarm occurs when there is a hardware failure in the GQAM modulator. When this condition exists, there is a potential for loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the GQAM modulator that is sending this alarm.

Front Panel Message

Hardware error

Possible Cause(s)

A hardware failure occurred.

Check and Correct

- 1 Power down and then power up the GQAM modulator using the on/off rocker-type switch on the back panel, or reset the GQAM modulator from the EC.
- 2 Replace the GQAM modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the GQAM modulator.
- 3 If the alarm continues to occur, contact Cisco Services for further assistance.

GQAM Modulator Alarm ID 89 (59 Hex)

The **Runtime Error** alarm displays when low-level software errors occur in the GQAM modulator. When this condition exists, there is a potential for loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the GQAM modulator that is sending this alarm.

Front Panel Message

Runtime error

Possible Cause(s)

Low-level software errors occurred.

Check and Correct

- 1 If this alarm continues to occur, power down and then power up the GQAM modulator using the on/off rocker- type switch on the back panel, or reset the GQAM modulator from the EC.
- 2 If resetting the GQAM modulator does not solve the problem, contact Cisco Services for further assistance.

GQAM Modulator Alarm ID 90 (5A Hex)

The **Craft Event Change** status event occurs when a user or a system operator uses the craft port to view or change the settings on the GQAM modulator. There is a potential for loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the GQAM modulator that is sending this event.

Front Panel Message

Craft change

Possible Cause(s)

A user or a system operator viewed or changed the settings on the GQAM modulator from the craft port.

Check and Correct

- 1 Check to see if any settings were changed.
- 2 Are all services functioning correctly?
 - If **yes**, no further action is required.
 - If **no**, go to step 3
- 3 Restore the settings to the previous configuration.
- 4 Power down and then power up the GQAM modulator using the on/off rocker-type switch on the back panel, or reset the GQAM modulator from the EC to restore the previous configuration.
- 5 If resetting the GQAM modulator does not solve the problem, contact Cisco Services for further assistance.

GQAM Modulator Alarm ID 91 (5B Hex)

The **Front Panel Event Change** status event occurs when a user or a system operator uses the front panel keys to change the settings on the GQAM modulator. There is a potential for loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the GQAM modulator that is sending this event.

Front Panel Message

Front panel change

Possible Cause(s)

A user or a system operator changed the settings on the GQAM modulator using the front panel keys.

Check and Correct

- 1 Verify what settings were changed.
- 2 Are all services functioning correctly?
 - If **yes**, no further action is required.
 - If **no**, go to step 3.
- 3 Restore the settings to the previous configuration.
- 4 Power down and then power up the GQAM modulator using the on/off rocker-type switch on the back panel, or reset the GQAM modulator from the EC to restore the previous configuration.
- 5 If resetting the GQAM modulator does not solve the problem, contact Cisco Services for further assistance.

GQAM Modulator Alarm ID 92 (5C Hex)

The **OUT 1 FIFO Overflow** alarm occurs when there is a FIFO overflow at output Channel 1 on the GQAM modulator, and packet data is lost. There is a low potential for loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the GQAM modulator that is sending this alarm.

Note: This alarm is self-clearing and may be intermittent. Single instances of this alarm that clear automatically and that do not reappear are not a cause for concern.

Front Panel Message

OUT1 FIFO Overflow

Possible Cause(s)

- The data rate as defined from the EC for the GQAM modulator sessions is too low, which also means that the data rate of the ASI input to the GQAM modulator is too high.
- There are too many sessions defined for the GQAM modulator from the EC.
- The modulation mode is incorrect.
- A hardware problem occurred.

Check and Correct

Data rate is too low

- 1 Reduce the amount of incoming data.
- 2 Reduce the amount of data added to the stream.
- 3 Increase the GQAM modulation mode.
- 4 Verify and correct session rate targets and threshold values

Too many sessions defined

Reduce the total number of MPEG programs by deleting sessions.

Modulation mode is incorrect

Verify and correct the modulation mode.

Hardware problem

- 1 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 2 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 3 If the alarm continues to occur, contact Cisco Services for further assistance.

GQAM Modulator Alarm ID 93 (5D Hex)

The **OUT 2 FIFO Overflow** alarm occurs when there is a FIFO overflow at output Channel 2 on the GQAM modulator, and packet data is lost. There is a low potential for loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the GQAM modulator that is sending this alarm.

Note: This alarm is self-clearing and may be intermittent. Single instances of this alarm that clear automatically and that do not reappear are not a cause for concern.

Front Panel Message

OUT2 FIFO Overflow

Possible Cause(s)

- The data rate as defined from the EC for the GQAM modulator sessions is too low, which also means that the data rate of the ASI input to the GQAM modulator is too high.
- There are too many sessions defined for the GQAM modulator from the EC.
- The modulation mode is incorrect
- A hardware problem occurred.

Check and Correct

Data rate is too low

- 1 Reduce the amount of incoming data.
- 2 Reduce the amount of data added to the stream.
- 3 Increase the GQAM modulation mode.
- 4 Verify and correct session rate targets and threshold values.

Too many sessions defined

Reduce the total number of MPEG programs by deleting sessions.

Modulation mode is incorrect

Verify and correct the modulation mode.

Hardware problem

- 1 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 2 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 3 If the alarm continues to occur, contact Cisco Services for further assistance.

GQAM Modulator Alarm ID 94 (5E Hex)

The **OUT 3 FIFO Overflow** alarm occurs when there is a FIFO overflow at output Channel 3 on the GQAM modulator, and packet data is lost. There is a low potential for loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the GQAM modulator that is sending this alarm.

Note: This alarm is self-clearing and may be intermittent. Single instances of this alarm that clear automatically and that do not reappear are not a cause for concern.

Front Panel Message

OUT3 FIFO Overflow

Possible Cause(s)

- The data rate as defined from the EC for the GQAM modulator sessions is too low, which also means that the data rate of the ASI input to the GQAM modulator is too high.
- There are too many sessions defined for the GQAM modulator from the EC.
- The modulation mode is incorrect.
- A hardware problem occurred.

Check and Correct

Data rate is too low

- 1 Reduce the amount of incoming data.
- 2 Reduce the amount of data added to the stream.
- 3 Increase the GQAM modulation mode.
- 4 Verify and correct session rate targets and threshold values.

Too many sessions defined

Reduce the total number of MPEG programs by deleting sessions.

Modulation mode is incorrect

Verify and correct the modulation mode.

Hardware problem

- 1 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 2 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 3 If the alarm continues to occur, contact Cisco Services for further assistance.

GQAM Modulator Alarm ID 95 (5F Hex)

The **OUT 4 FIFO Overflow** alarm occurs when there is a FIFO overflow at output Channel 4 on the GQAM modulator, and packet data is lost. There is a low potential for loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the GQAM modulator that is sending this alarm.

Note: This alarm is self-clearing and may be intermittent. Single instances of this alarm that clear automatically and that do not reappear are not a cause for concern.

Front Panel Message

OUT4 FIFO Overflow

Possible Cause(s)

- The data rate as defined from the EC for the GQAM modulator sessions is too low, which also means that the data rate of the ASI input to the GQAM modulator is too high.
- There are too many sessions defined for the GQAM modulator from the EC.
- The modulation mode is incorrect.
- A hardware problem occurred.

Check and Correct

Data rate is too low

- 1 Reduce the amount of incoming data.
- 2 Reduce the amount of data added to the stream.
- 3 Increase the GQAM modulation mode.
- 4 Verify and correct session rate targets and threshold values.

Too many sessions defined

Reduce the total number of MPEG programs by deleting sessions.

Modulation mode is incorrect

Verify and correct the modulation mode.

Hardware problem

- 1 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 2 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 3 If the alarm continues to occur, contact Cisco Services for further assistance.

GQAM Modulator Alarm ID 96 (60 Hex)

The **OUT 5 FIFO Overflow** alarm occurs when there is a FIFO overflow at output Channel 5 on the GQAM modulator, and packet data is lost. There is a low potential for loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the GQAM modulator that is sending this alarm.

Note: This alarm is self-clearing and may be intermittent. Single instances of this alarm that clear automatically and that do not reappear are not a cause for concern.

Front Panel Message

OUT5 FIFO Overflow

Possible Cause(s)

- The data rate as defined from the EC for the GQAM modulator sessions is too low, which also means that the data rate of the ASI input to the GQAM modulator is too high.
- There are too many sessions defined for the GQAM modulator from the EC.
- The modulation mode is incorrect.
- A hardware problem occurred.

Check and Correct

Data rate is too low

- 1 Reduce the amount of incoming data.
- 2 Reduce the amount of data added to the stream.
- 3 Increase the GQAM modulation mode.
- 4 Verify and correct session rate targets and threshold values.

Too many sessions defined

Reduce the total number of MPEG programs by deleting sessions.

Modulation mode is incorrect

Verify and correct the modulation mode.

Hardware problem

- 1 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 2 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 3 If the alarm continues to occur, contact Cisco Services for further assistance.

GQAM Modulator Alarm ID 97 (61 Hex)

The **OUT 6 FIFO Overflow** alarm occurs when there is a FIFO overflow at output Channel 6 on the GQAM modulator, and packet data is lost. There is a low potential for loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the GQAM modulator that is sending this alarm.

Note: This alarm is self-clearing and may be intermittent. Single instances of this alarm that clear automatically and that do not reappear are not a cause for concern.

Front Panel Message

OUT6 FIFO Overflow

Possible Cause(s)

- The data rate as defined from the EC for the GQAM modulator sessions is too low, which also means that the data rate of the ASI input to the GQAM modulator is too high.
- There are too many sessions defined for the GQAM modulator from the EC.
- The modulation mode is incorrect.
- A hardware problem occurred.

Check and Correct

Data rate is too low

- 1 Reduce the amount of incoming data.
- 2 Reduce the amount of data added to the stream.
- 3 Increase the GQAM modulation mode.
- 4 Verify and correct session rate targets and threshold values.

Too many sessions defined

Reduce the total number of MPEG programs by deleting sessions.

Modulation mode is incorrect

Verify and correct the modulation mode.

Hardware problem

- 1 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 2 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 3 If the alarm continues to occur, contact Cisco Services for further assistance.

GQAM Modulator Alarm ID 98 (62 Hex)

The **OUT 7 FIFO Overflow** alarm occurs when there is a FIFO overflow at output Channel 7 on the GQAM modulator, and packet data is lost. There is a low potential for loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the GQAM modulator that is sending this alarm.

Note: This alarm is self-clearing and may be intermittent. Single instances of this alarm that clear automatically and that do not reappear are not a cause for concern.

Front Panel Message

OUT7 FIFO Overflow

Possible Cause(s)

- The data rate as defined from the EC for the GQAM modulator sessions is too low, which also means that the data rate of the ASI input to the GQAM modulator is too high.
- There are too many sessions defined for the GQAM modulator from the EC.
- The modulation mode is incorrect.
- A hardware problem occurred.

Check and Correct

Data rate is too low

- 1 Reduce the amount of incoming data.
- 2 Reduce the amount of data added to the stream.
- 3 Increase the GQAM modulation mode.
- 4 Verify and correct session rate targets and threshold values.

Too many sessions defined

Reduce the total number of MPEG programs by deleting sessions.

Modulation mode is incorrect

Verify and correct the modulation mode.

Hardware problem

- 1 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 2 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 3 If the alarm continues to occur, contact Cisco Services for further assistance.

GQAM Modulator Alarm ID 99 (63 Hex)

The **OUT 8 FIFO Overflow** alarm occurs when there is a FIFO overflow at output Channel 8 on the GQAM modulator, and packet data is lost. There is a low potential for loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the GQAM modulator that is sending this alarm.

Note: This alarm is self-clearing and may be intermittent. Single instances of this alarm that clear automatically and that do not reappear are not a cause for concern.

Front Panel Message

OUT8 FIFO Overflow

Possible Cause(s)

- The data rate as defined from the EC for the GQAM modulator sessions is too low, which also means that the data rate of the ASI input to the GQAM modulator is too high.
- There are too many sessions defined for the GQAM modulator from the EC.
- The modulation mode is incorrect.
- A hardware problem occurred.

Check and Correct

Data rate is too low

- 1 Reduce the amount of incoming data.
- 2 Reduce the amount of data added to the stream.
- 3 Increase the GQAM modulation mode.
- 4 Verify and correct session rate targets and threshold values.

Too many sessions defined

Reduce the total number of MPEG programs by deleting sessions.

Modulation mode is incorrect

Verify and correct the modulation mode.

Hardware problem

- 1 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 2 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 3 If the alarm continues to occur, contact Cisco Services for further assistance.

GQAM Modulator Alarm ID 100 (64 Hex)

The **OUT 9 FIFO Overflow** alarm occurs when there is a FIFO overflow at output Channel 9 on the GQAM modulator, and packet data is lost. There is a low potential for loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the GQAM modulator that is sending this alarm.

Note: This alarm is self-clearing and may be intermittent. Single instances of this alarm that clear automatically and that do not reappear are not a cause for concern.

Front Panel Message

OUT9 FIFO Overflow

Possible Cause(s)

- The data rate as defined from the EC for the GQAM modulator sessions is too low, which also means that the data rate of the ASI input to the GQAM modulator is too high.
- There are too many sessions defined for the GQAM modulator from the EC.
- The modulation mode is incorrect.
- A hardware problem occurred.

Check and Correct

Data rate is too low

- 1 Reduce the amount of incoming data.
- 2 Reduce the amount of data added to the stream.
- 3 Increase the GQAM modulation mode.
- 4 Verify and correct session rate targets and threshold values.

Too many sessions defined

Reduce the total number of MPEG programs by deleting sessions.

Modulation mode is incorrect

Verify and correct the modulation mode.

Hardware problem

- 1 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 2 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 3 If the alarm continues to occur, contact Cisco Services for further assistance.

GQAM Modulator Alarm ID 101 (65 Hex)

The **OUT 10 FIFO Overflow** alarm occurs when there is a FIFO overflow at output Channel 10 on the GQAM modulator, and packet data is lost. There is a low potential for loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the GQAM modulator that is sending this alarm.

Note: This alarm is self-clearing and may be intermittent. Single instances of this alarm that clear automatically and that do not reappear are not a cause for concern.

Front Panel Message

OUT10 FIFO Overflow

Possible Cause(s)

- The data rate as defined from the EC for the GQAM modulator sessions is too low, which also means that the data rate of the ASI input to the GQAM modulator is too high.
- There are too many sessions defined for the GQAM modulator from the EC.
- The modulation mode is incorrect.
- A hardware problem occurred.

Check and Correct

Data rate is too low

- 1 Reduce the amount of incoming data.
- 2 Reduce the amount of data added to the stream.
- 3 Increase the GQAM modulation mode.
- 4 Verify and correct session rate targets and threshold values.

Too many sessions defined

Reduce the total number of MPEG programs by deleting sessions.

Modulation mode is incorrect

Verify and correct the modulation mode.

Hardware problem

- 1 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 2 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 3 If the alarm continues to occur, contact Cisco Services for further assistance.

GQAM Modulator Alarm ID 102 (66 Hex)

The **OUT 11 FIFO Overflow** alarm occurs when there is a FIFO overflow at output Channel 11 on the GQAM modulator, and packet data is lost. There is a low potential for loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the GQAM modulator that is sending this alarm.

Note: This alarm is self-clearing and may be intermittent. Single instances of this alarm that clear automatically and that do not reappear are not a cause for concern.

Front Panel Message

OUT11 FIFO Overflow

Possible Cause(s)

- The data rate as defined from the EC for the GQAM modulator sessions is too low, which also means that the data rate of the ASI input to the GQAM modulator is too high.
- There are too many sessions defined for the GQAM modulator from the EC.
- The modulation mode is incorrect.
- A hardware problem occurred.

Check and Correct

Data rate is too low

- 1 Reduce the amount of incoming data.
- 2 Reduce the amount of data added to the stream.
- 3 Increase the GQAM modulation mode.
- 4 Verify and correct session rate targets and threshold values.

Too many sessions defined

Reduce the total number of MPEG programs by deleting sessions.

Modulation mode is incorrect

Verify and correct the modulation mode.

Hardware problem

- 1 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 2 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 3 If the alarm continues to occur, contact Cisco Services for further assistance.

GQAM Modulator Alarm ID 103 (67 Hex)

The **OUT 12 FIFO Overflow** alarm occurs when there is a FIFO overflow at output Channel 12 on the GQAM modulator, and packet data is lost. There is a low potential for loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the GQAM modulator that is sending this alarm.

Note: This alarm is self-clearing and may be intermittent. Single instances of this alarm that clear automatically and that do not reappear are not a cause for concern.

Front Panel Message

OUT12 FIFO Overflow

Possible Cause(s)

- The data rate as defined from the EC for the GQAM modulator sessions is too low, which also means that the data rate of the ASI input to the GQAM modulator is too high.
- There are too many sessions defined for the GQAM modulator from the EC.
- The modulation mode is incorrect.
- A hardware problem occurred.

Check and Correct

Data rate is too low

- 1 Reduce the amount of incoming data.
- 2 Reduce the amount of data added to the stream.
- 3 Increase the GQAM modulation mode.
- 4 Verify and correct session rate targets and threshold values.

Too many sessions defined

Reduce the total number of MPEG programs by deleting sessions.

Modulation mode is incorrect

Verify and correct the modulation mode.

Hardware problem

- 1 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 2 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 3 If the alarm continues to occur, contact Cisco Services for further assistance.

GQAM Modulator Alarm ID 104 (68 Hex)

The **OUT 13 FIFO Overflow** alarm occurs when there is a FIFO overflow at output Channel 13 on the GQAM modulator, and packet data is lost. There is a low potential for loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the GQAM modulator that is sending this alarm.

Note: This alarm is self-clearing and may be intermittent. Single instances of this alarm that clear automatically and that do not reappear are not a cause for concern.

Front Panel Message

OUT13 FIFO Overflow

Possible Cause(s)

- The data rate as defined from the EC for the GQAM modulator sessions is too low, which also means that the data rate of the ASI input to the GQAM modulator is too high.
- There are too many sessions defined for the GQAM modulator from the EC.
- The modulation mode is incorrect.
- A hardware problem occurred.

Check and Correct

Data rate is too low

- 1 Reduce the amount of incoming data.
- 2 Reduce the amount of data added to the stream.
- 3 Increase the GQAM modulation mode.
- 4 Verify and correct session rate targets and threshold values.

Too many sessions defined

Reduce the total number of MPEG programs by deleting sessions.

Modulation mode is incorrect

Verify and correct the modulation mode.

Hardware problem

- 1 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 2 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 3 If the alarm continues to occur, contact Cisco Services for further assistance.

GQAM Modulator Alarm ID 105 (69 Hex)

The **OUT 14 FIFO Overflow** alarm occurs when there is a FIFO overflow at output Channel 14 on the GQAM modulator, and packet data is lost. There is a low potential for loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the GQAM modulator that is sending this alarm.

Note: This alarm is self-clearing and may be intermittent. Single instances of this alarm that clear automatically and that do not reappear are not a cause for concern.

Front Panel Message

OUT14 FIFO Overflow

Possible Cause(s)

- The data rate as defined from the EC for the GQAM modulator sessions is too low, which also means that the data rate of the ASI input to the GQAM modulator is too high.
- There are too many sessions defined for the GQAM modulator from the EC.
- The modulation mode is incorrect.
- A hardware problem occurred.

Check and Correct

Data rate is too low

- 1 Reduce the amount of incoming data.
- 2 Reduce the amount of data added to the stream.
- 3 Increase the GQAM modulation mode.
- 4 Verify and correct session rate targets and threshold values.

Too many sessions defined

Reduce the total number of MPEG programs by deleting sessions.

Modulation mode is incorrect

Verify and correct the modulation mode.

Hardware problem

- 1 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 2 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 3 If the alarm continues to occur, contact Cisco Services for further assistance.

GQAM Modulator Alarm ID 106 (6A Hex)

The **OUT 15 FIFO Overflow** alarm occurs when there is a FIFO overflow at output Channel 15 on the GQAM modulator, and packet data is lost. There is a low potential for loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the GQAM modulator that is sending this alarm.

Note: This alarm is self-clearing and may be intermittent. Single instances of this alarm that clear automatically and that do not reappear are not a cause for concern.

Front Panel Message

OUT15 FIFO Overflow

Possible Cause(s)

- The data rate as defined from the EC for the GQAM modulator sessions is too low, which also means that the data rate of the ASI input to the GQAM modulator is too high.
- There are too many sessions defined for the GQAM modulator from the EC.
- The modulation mode is incorrect.
- A hardware problem occurred.

Check and Correct

Data rate is too low

- 1 Reduce the amount of incoming data.
- 2 Reduce the amount of data added to the stream.
- 3 Increase the GQAM modulation mode.
- 4 Verify and correct session rate targets and threshold values.

Too many sessions defined

Reduce the total number of MPEG programs by deleting sessions.

Modulation mode is incorrect

Verify and correct the modulation mode.

Hardware problem

- 1 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 2 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 3 If the alarm continues to occur, contact Cisco Services for further assistance.

GQAM Modulator Alarm ID 107 (6B Hex)

The **OUT 16 FIFO Overflow** alarm occurs when there is a FIFO overflow at output Channel 16 on the GQAM modulator, and packet data is lost. There is a low potential for loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the GQAM modulator that is sending this alarm.

Note: This alarm is self-clearing and may be intermittent. Single instances of this alarm that clear automatically and that do not reappear are not a cause for concern.

Front Panel Message

OUT16 FIFO Overflow

Possible Cause(s)

- The data rate as defined from the EC for the GQAM modulator sessions is too low, which also means that the data rate of the ASI input to the GQAM modulator is too high.
- There are too many sessions defined for the GQAM modulator from the EC.
- The modulation mode is incorrect.
- A hardware problem occurred.

Check and Correct

Data rate is too low

- 1 Reduce the amount of incoming data.
- 2 Reduce the amount of data added to the stream.
- 3 Increase the GQAM modulation mode.
- 4 Verify and correct session rate targets and threshold values.

Too many sessions defined

Reduce the total number of MPEG programs by deleting sessions.

Modulation mode is incorrect

Verify and correct the modulation mode.

Hardware problem

- 1 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 2 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 3 If the alarm continues to occur, contact Cisco Services for further assistance.

GQAM Modulator Alarm ID 108 (6C Hex)

The **Fan Failure #1** alarm occurs when ventilation fan rotor #1 on the side panel of the GQAM modulator fails. You must replace the entire dual fan unit immediately to prevent the GQAM from overheating.

Note: There are three dual fan units on the side panel of the GQAM modulator. Each of these fan units contains two fan rotors. You must replace the entire fan unit if one of the fan rotors should fail.

Front Panel Message

Fan Failure #1

Possible Cause(s)

One of the fan rotors failed.

Check and Correct

Replace the dual fan unit that has failed. Contact your Cisco North American Marketing Manager to arrange for a genuine replacement fan unit. To properly install the fan unit, follow the installation instructions that ship with the replacement fan unit.

GQAM Modulator Alarm ID 109 (6D Hex)

The **Fan Failure #2** alarm occurs when ventilation fan rotor #2 on the side panel of the GQAM modulator fails. You must replace the entire dual fan unit immediately to prevent the GQAM from overheating.

Note: There are three dual fan units on the side panel of the GQAM modulator. Each of these fan units contains two fan rotors. You must replace the entire fan unit if one of the fan rotors should fail.

Front Panel Message

Fan Failure #2

Possible Cause(s)

One of the fan rotors failed.

Check and Correct

Replace the dual fan unit that has failed. Contact your Cisco North American Marketing Manager to arrange for a genuine replacement fan unit. To properly install the fan unit, follow the installation instructions that ship with the replacement fan.

GQAM Modulator Alarm ID 110 (6E Hex)

The **Fan Failure #3** alarm occurs when ventilation fan rotor #3 on the side panel of the GQAM modulator fails. You must replace the entire dual fan unit immediately to prevent the GQAM from overheating.

Note: There are three dual fan units on the side panel of the GQAM modulator. Each of these fan units contains two fan rotors. You must replace the entire fan unit if one of the fan rotors should fail.

Front Panel Message

Fan Failure #3

Possible Cause(s)

One of the fan rotors failed.

Check and Correct

Replace the dual fan unit that has failed. Contact your Cisco North American Marketing Manager to arrange for a genuine replacement fan unit . To properly install the fan unit, follow the installation instructions that ship with the replacement fan unit.

GQAM Modulator Alarm ID 111 (6F Hex)

The **Fan Failure #4** alarm occurs when ventilation fan rotor #4 on the side panel of the GQAM modulator fails. You must replace the entire dual fan unit immediately to prevent the GQAM from overheating.

Note: There are three dual fan units on the side panel of the GQAM modulator. Each of these fan units contains two fan rotors. You must replace the entire fan unit if one of the fan rotors should fail.

Front Panel Message

Fan Failure #4

Possible Cause(s)

One of the fan rotors failed.

Check and Correct

Replace the dual fan unit that has failed. Contact your Cisco North American Marketing Manager to arrange for a genuine replacement fan unit. To properly install the fan unit, follow the installation instructions that ship with the replacement fan unit.

GQAM Modulator Alarm ID 112 (70 Hex)

The **Fan Failure #5** alarm occurs when ventilation fan rotor #5 on the side panel of the GQAM modulator fails. You must replace the entire dual fan unit immediately to prevent the GQAM from overheating.

Note: There are three dual fan units on the side panel of the GQAM modulator. Each of these fan units contains two fan rotors. You must replace the entire fan unit if one of the fan rotors should fail.

Front Panel Message

Fan Failure #5

Possible Cause(s)

One of the fan rotors failed.

Check and Correct

Replace the dual fan unit that has failed. Contact your Cisco North American Marketing Manager to arrange for a genuine replacement fan unit. To properly install the fan unit, follow the installation instructions that ship with the replacement fan unit.

GQAM Modulator Alarm ID 113 (71 Hex)

The **Fan Failure #6** alarm occurs when ventilation fan rotor #6 on the side panel of the GQAM modulator fails. You must replace the entire dual fan unit immediately to prevent the GQAM from overheating.

Note: There are three dual fan units on the side panel of the GQAM modulator. Each of these fan units contains two fan rotors. You must replace the entire fan unit if one of the fan rotors should fail.

Front Panel Message

Fan Failure #6

Possible Cause(s)

One of the fan rotors failed.

Check and Correct

Replace the dual fan unit that has failed. Contact your Cisco North American Marketing Manager to arrange for a genuine replacement fan unit. To properly install the fan unit, follow the installation instructions that ship with the replacement fan unit.

GQAM Modulator Alarm ID 256 (100 Hex) through Alarm ID 1247 (4DF Hex)

The **Session Data Error** alarm occurs when the GQAM modulator detects a session data error and indicates one of the following conditions:

- Underflow and overflow errors indicate that the data flow for the session is more or less than what has been defined by the EC for the session.
Important! The default threshold for the underflow and overflow alarms is zero. Note that the same threshold parameter is utilized for determining both underflow and overflow. The algorithm for determining underflow/overflow is as follows:
- When the threshold value is not provisioned by a management entity, the threshold value is 0 and the UNDERFLOW alarm will occur if the session's data rate falls below 1 bit per second (bps) (i.e., either equal to 0 bps or a fractional value that is less than 1 bps). In other words, the Overflow alarm is essentially disabled.
- When a management entity provisions the alarm with a non-zero threshold value, the UNDERFLOW alarm occurs when the measured session data rate falls below (sessionRate - threshold) and the OVERFLOW alarm occurs when the measured session data rate exceeds (sessionRate + threshold).
Note: sessionRate is the rate that was specified createSession request.
- PID enable errors indicate that a PID for this session is not enabled in the GQAM modulator.
Note: A PID is contained in the MPEG header to link MPEG packets together.
- Continuity error.
- PLL unlocked
- Excess glue frame events

Alarm IDs 256 (decimal) through 1247 (decimal) represent Session Data alarms. Sessions correspond to MPEG programs. The GQAM modulator has four labeled RF output ports. Each of these output ports carries four QAM modulated channels for a total of 16 QAM modulated RF output channels. Each QAM modulated channel can support 62 sessions for a total of 992 sessions per GQAM modulator. While each GQAM output can support 64 rate cells, 62 of the rate cells are for sessions, and 2 of the rate cells are for table insertion overhead (for example, SI), so the DHCTs can find their channel information and ECMs to tell the DHCTs what entitlements are active on the current content. Each of these sessions will generate a unique Alarm ID when a Session Data Error occurs for that session.

Chapter 3 GQAM Modulator Alarms

Session data alarms for internal session indices 0 through 991 on the GQAM modulator are mapped to session data error Alarm IDs 256 (decimal) through 1247 (decimal) though the reserved range in the code is up to 1279 (decimal).

Important! The **Additional Information** field in the Alarm Manager window displays the Session ID number, the Input port number, the Output port number, and the Cause Code.

There is potential loss of programming content, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the GQAM modulator that is sending this alarm.

Front Panel Message

Session xxx data error

Note: Session front panel messages display a number representing the internal session number used by the GQAM modulator. The number is between 000 and 991, and is shown as a decimal value.

Possible Cause(s)

The data flow for the session is lesser than or greater than what is defined by the EC for the session. This indicates one or more of the following underflow and overflow conditions:

- Cause Code 1 - Underflow conditions - The session data rate for this session drops to 0 (zero) or is less than expected.
Important! The session rate dropping to 0 (zero) triggers an underflow alarm, but is not the result of a loss of signal condition. When a loss of signal occurs, the underflow alarm is not reported. This prevents the system from being overwhelmed with a large number of session data alarms. Alarms that occur as a result of higher level alarms are not reported.
- Cause Code 2 - Overflow conditions - The data rate for this session exceeds the provisioned data rate.
- Cause Code 3 - PID enable error - A PID that should be enabled is not enabled in the GQAM modulator.
- Cause Code 6 - Continuity error - This alarm identifies the specific session on which the Input Port (1-5) continuity error alarm occurred
- Cause Code 7 - PLL unlocked - The phase lock loop is unlocked for the given session.

GQAM Modulator Alarm ID 256 (100 Hex) through Alarm ID 1247 (4DF Hex)

- Cause Code 8 - Excess glue frame events - Glue frames prevent macroblocking. Excess glue frame events indicate that the associated output port is receiving too much data. When the MPEG engine in the GQAM modulator nears full output capacity, it begins to selectively choose video PIDs on which it will issue a "freeze frame" code in the MPEG video stream for that program. Then the device drops the video packets for that session momentarily. This will happen only for sessions for which glue framing was enabled when the session was created. If this alarm occurs frequently, it is a signal that the output QAM carrying that session contains too much data.

Check and Correct

Overflow and underflow conditions

- 1 Verify and correct any session setup problems, including the session rate target values.
Note: Select data rates that you believe the program should not exceed.
- 2 For the overflow condition, teardown, rebuild, and then restart the session using a higher bandwidth.
- 3 If the session setup data is correct, the data may be corrupt.
- 4 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 5 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report. If you cannot resolve these issues, contact Cisco Services.

PID enable issues

- If this alarm occurs with this Cause Code and then quickly clears, it is not a cause for concern.
- If the alarm does not quickly clear, verify and enable the PID in the GQAM modulator.

Continuity error

Contact Cisco Services for further assistance.

PLL unlocked

Contact Cisco Services for further assistance.

Excess glue frame events

Reallocate the session from the QAM modulator that appears to have too many sessions to another QAM modulator on the same GQAM modulator or to another GQAM modulator.

GQAM Modulator Alarm ID 1280 (500 Hex) through Alarm ID 2271 (8DF Hex)

The **Session Program Error** alarm occurs when there are errors or other problems in the input source for the session.

Alarm IDs 1280 (decimal) through 2271 (decimal) represent Session Program Error alarms. Sessions correspond to MPEG programs. The GQAM modulator has four labeled RF output ports. Each of these output ports carries four QAM modulated channels for a total of 16 QAM modulated RF output channels. Each QAM modulated channel can support 62 sessions for a total of 992 sessions per GQAM modulator. While each GQAM output can support 64 rate cells, 62 of the rate cells are for sessions, and 2 of the rate cells are for table insertion overhead (for example, SI), so the DHCTs can find their channel information and ECMs to tell the DHCTs what entitlements are active on the current content. Each of these sessions will generate a unique Alarm ID when a Session Program Error occurs for that session.

Session program alarms for internal session indices 0 through 991 on the GQAM modulator are mapped to session program Alarm IDs 1280 (decimal) through 2271 (decimal) though the reserved range in the code is up to 2303 (decimal).

There is a potential for loss of programming content, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the GQAM modulator that is sending this alarm.

Important! The **Additional Information** field in the Alarm Manager window displays the Session ID number, the Input port number, the Output port number, and the Cause Code.

Front Panel Message

Session xxx prog error

Note: Session front panel messages display a number representing the internal session number used by the GQAM modulator. The number is between 000 and 991, and is shown as a decimal value.

Possible Cause(s)

- Cause Code 1 - A CRC error was detected on a PMT.
- Cause Code 2 - A new PMT was detected.
- Cause Code 3 - An attempt to create a session failed.
- The PSI table data for the session contains errors.

Check and Correct

CRC error detected

Delete the session

GQAM Modulator Alarm ID 1280 (500 Hex) through Alarm ID 2271 (8DF Hex)

New PMT detected

This is for information only. No action is required.

Create a session failed

Teardown and rebuild the session.

PSI table contains errors

Check the upstream MPEG input sources connected to the GQAM modulator.

GQAM Modulator Alarm ID 2304 (900 Hex) through Alarm ID 3295 (CDF Hex)

The **Session Conditional Access Error** alarm occurs when the GQAM modulator detects an error in the CA encryption for a session. This alarm indicates that the signal is being transmitted in the clear, when it should be encrypted.

Alarm IDs 2304 (decimal) through 3295 (decimal) represent Session Conditional Access alarms. Sessions correspond to MPEG programs. The GQAM modulator has four labeled RF output ports. Each of these output ports carries four QAM modulated channels for a total of 16 QAM modulated RF output channels. Each QAM modulated channel can support 62 sessions for a total of 992 sessions per GQAM modulator. While each GQAM output can support 64 rate cells, 62 of the rate cells are for sessions, and 2 of the rate cells are for table insertion overhead (for example, SI), so the DHCTs can find their channel information and ECMs to tell the DHCTs what entitlements are active on the current content. Each of these sessions will generate a unique Alarm ID when a Session Conditional Access Error occurs.

Session CA alarms for internal session indices 0 through 991 on the GQAM modulator are mapped to the session CA alarm IDs 2304 (decimal) through 3295 (decimal) though the reserved range in the code is up to 3327 (decimal).

Important! When this condition exists, certain sessions may be broadcast without encryption, impacting potential pay-per-view and subscription revenues, and resulting in some subscribers receiving channels and services they do not want.

There is a potential for loss of programming content, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the GQAM modulator that is sending this alarm.

Important! The Additional Information field in the Alarm Manager window displays the Session ID number, the Input port number, and the Output port number.

Front Panel Message

Session xxx ca error

Note: Session front panel messages display a number representing the internal session number used by the GQAM modulator. The number is between 000 and 991, and is shown as a decimal value.

Possible Cause(s)

- CA failed.
- The CA settings are improper.
- A bad ISK VOD session.
- A hardware failure occurred.

GQAM Modulator Alarm ID 2304 (900 Hex) through Alarm ID 3295 (CDF Hex)

Check and Correct

CA failed

Delete the failed session.

CA settings improper

Check and correct the CA settings on the EC.

Bad ISK message

- 1 Troubleshoot CA on the EC.
- 2 Contact Cisco Services.

Hardware failure

- 1 Replace the GQAM modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the GQAM modulator.
- 2 Contact Cisco Services for further assistance.

GQAM Modulator Alarm ID 3328 (D00 Hex) through Alarm ID 4351 (10FF Hex)

The **Session NP Gigabit Ethernet Error** alarm occurs when the GQAM modulator detects an error in the...

Alarm IDs 3328 (decimal) through 4319 (decimal) represent Session NP Gigabit Ethernet alarms. Sessions correspond to MPEG programs. The GQAM modulator has four labeled RF output ports. Each of these output ports carries four QAM modulated channels for a total of 16 QAM modulated RF output channels. Each QAM modulated channel can support 62 sessions for a total of 992 sessions per GQAM modulator. While each GQAM output can support 64 rate cells, 62 of the rate cells are for sessions, and 2 of the rate cells are for table insertion overhead (for example, SI), so the DHCTs can find their channel information and ECMs to tell the DHCTs what entitlements are active on the current content. Each of these sessions will generate a unique Alarm ID when a Session NP Gigabit Ethernet Error occurs.

Session NP Gigabit Ethernet alarms for internal session indices 0 through 991 on the GQAM modulator are mapped to the session NP Gigabit Ethernet alarm IDs 3328 (decimal) through 4319 (decimal) though the reserved range in the code is up to 4351 (decimal).

There is a potential for loss of programming content, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the GQAM modulator that is sending this alarm.

Important! The Additional Information field in the Alarm Manager window displays the Session ID number, the Input port number, the Output port number, and the Cause Code.

Front Panel Message

Session xxxx GE error

Note: Session front panel messages display a number representing the internal session number used by the GQAM modulator. The number is between 000 and 991, and is shown as a decimal value.

4

Netcrypt Alarms

Introduction

Alarm levels for the Netcrypt are classified as major, minor, and status alarms. Each level is described as follows:

Major Alarms - A major alarm indicates a fatal error, that is, a complete loss of functionality. Major alarms occur for hardware or software conditions that indicate a serious disruption of service or the malfunctioning or failure of important circuits. These situations require the immediate response of the technician to restore or maintain system operability. The front panel of the Netcrypt contains a MAJOR LED to alert the operator that a major alarm is pending.

Minor Alarms - A minor alarm indicates a non-fatal error condition. The Netcrypt may continue to operate with some loss of functionality. The front panel of the Netcrypt contains a MINOR LED to alert the operator that a minor alarm is pending.

Status Alarms - The status alarm indicates that some state in the Netcrypt has changed. These are generally one-time events, such as a front panel event change. In this case, the alarm is issued with the level "status" each time you press the ENTER key on the front panel of the Netcrypt. Status alarms might or might not affect Netcrypt functionality.

Note: Status alarms alert the EC operator that possible changes are occurring at the Netcrypt site caused by someone operating the front panel keys or connecting to the craft port.

Netcrypt Alarm ID 0 (0 Hex)

The **Netcrypt Exceeded Max Temperature** minor alarm occurs when the internal temperature of the Netcrypt exceeds 70°C (158°F). A Netcrypt that is overheating could have minimal to severe impact on services. If the modulator fails due to overheating, there would be no services available from that Netcrypt device.

Front Panel Message

None

Possible Cause(s)

- The vents on the Netcrypt are blocked.
- The room temperature is too high.
- A fan failure occurred.
- A hardware failure occurred.

Check and Correct

Vents are blocked

Check and clear any obstructions from the vents.

Room temperature is too high

Check and repair or replace the heating/cooling equipment in the room.

Fan failure

Check and repair or replace the fan.

Hardware failure

- 1 Replace the Netcrypt if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the Netcrypt.
- 2 If the alarm condition continues to occur, contact Cisco Services.

Netcrypt Alarm ID 1 (1 Hex)

The Netcrypt **Input 1 MPEG Continuity Error** minor alarm occurs when individual MPEG packets become corrupted due to random noise in the network. Each MPEG packet has a section for continuity bits that should contain a sequential value. These MPEG continuity bits are used by the MPEG packet recipient to verify that the packets in an MPEG stream are received in the correct sequential order and to verify that no packet loss has occurred.

This alarm also occurs when the Netcrypt receives packets in the MPEG stream that do not contain MPEG continuity bits.

There is a potential for loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the Netcrypt that is sending this alarm.

Front Panel Message

None

Possible Cause(s)

- A cable is loose, disconnected, or defective.
- There are data errors on the satellite link.
- The rate of change of the IEC exceeds the allowed threshold.
- There is defective upstream equipment or failure on the input data link of the Netcrypt.
- There is defective local MPEG coding.
- The Netcrypt is defective.

Check and Correct

Loose, disconnected, or defective cables

Check for loose connections or defective cables, tighten any loose cable connections, connect any disconnected cables, and replace any defective cables.

Satellite link data errors

Contact your signal provider to verify if there are any problems with their satellite transmissions.

IEC errors

Clean up the MPEG signal input to the Netcrypt by checking the IRT, RTE, and MPEG encoder along with the GigE stream.

Chapter 4 Netcrypt Alarms

Defective upstream equipment

- 1 Check the upstream devices that are sending MPEG packets to the Netcrypt.
- 2 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of service.

Important!

- If the majority of MPEG packet alarms are occurring in a single Netcrypt, then that Netcrypt or its input should be the focus of the troubleshooting.
 - If the majority of MPEG packet alarms are occurring in more than one Netcrypt, then the troubleshooting should focus upstream on the device that is providing a common source of input to the Netcrypt with errors.
 - If the Netcrypt has a common device upstream, then that device is the most likely source of the packet errors
- 3 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
 - 4 If the alarm continues to occur, contact Cisco Services for further assistance.

Defective local MPEG coding

Check the local source devices that are providing MPEG content to the Netcrypt.

Netcrypt is defective

- 1 Replace the Netcrypt if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the Netcrypt.
- 2 If the alarm continues to occur, contact Cisco Services for further assistance.

Netcrypt Alarm ID 2 (2 Hex)

The Netcrypt **Input 1 MPEG Transport Error** minor alarm occurs when there is an error in the header of some of the MPEG packets received by the Netcrypt. There is a potential for loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the Netcrypt that is sending this alarm.

Note: This alarm is self-clearing and may be intermittent. Single instances of this alarm that clear automatically and that do not reappear are not a cause for concern.

Front Panel Message

None

Possible Cause(s)

There is an error in the header of an MPEG packet.

Check and Correct

- 1 Check the upstream devices that are sending MPEG packets to the input ports on the Netcrypt.
- 2 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 3 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 4 If the alarm continues to occur, contact Cisco Services for further assistance.

Netcrypt Alarm ID 3 (3 Hex)

The Netcrypt **Input 2 MPEG Continuity Error** minor alarm occurs when individual MPEG packets become corrupted due to random noise in the network. Each MPEG packet has a section for continuity bits that should contain a sequential value. These MPEG continuity bits are used by the MPEG packet recipient to verify that the packets in an MPEG stream are received in the correct sequential order and to verify that no packet loss has occurred.

This alarm also occurs when the Netcrypt receives packets in the MPEG stream that do not contain MPEG continuity bits.

There is a potential for loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the Netcrypt that is sending this alarm.

Front Panel Message

None

Possible Cause(s)

- A cable is loose, disconnected, or defective.
- There are data errors on the satellite link.
- The rate of change of the IEC exceeds the allowed threshold.
- There is defective upstream equipment or failure on the input data link of the Netcrypt.
- There is defective local MPEG coding.
- The Netcrypt is defective.

Check and Correct

Loose, disconnected, or defective cables

Check for loose connections or defective cables, tighten any loose cable connections, connect any disconnected cables, and replace any defective cables.

Satellite link data errors

Contact your signal provider to verify if there are any problems with their satellite transmissions.

IEC errors

Clean up the MPEG signal input to the Netcrypt by checking the IRT, RTE, and MPEG encoder along with the GigE stream.

Defective upstream equipment

- 1 Check the upstream devices that are sending MPEG packets to the Netcrypt.
- 2 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of service.

Important!

- If the majority of MPEG packet alarms are occurring in a single Netcrypt, then that Netcrypt or its input should be the focus of the troubleshooting.
 - If the majority of MPEG packet alarms are occurring in more than one Netcrypt, then the troubleshooting should focus upstream on the device that is providing a common source of input to the Netcrypt with errors.
 - If the Netcrypt has a common device upstream, then that device is the most likely source of the packet errors
- 3 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
 - 4 If the alarm continues to occur, contact Cisco Services for further assistance.

Defective local MPEG coding

Check the local source devices that are providing MPEG content to the Netcrypt.

Netcrypt is defective

- 1 Replace the Netcrypt if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the Netcrypt.
- 2 If the alarm continues to occur, contact Cisco Services for further assistance.

Netcrypt Alarm ID 4 (4 Hex)

The Netcrypt **Input 2 MPEG Transport Error** minor alarm occurs when there is an error in the header of some of the MPEG packets received by the Netcrypt. There is a potential for loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the Netcrypt that is sending this alarm.

Note: This alarm is self-clearing and may be intermittent. Single instances of this alarm that clear automatically and that do not reappear are not a cause for concern.

Front Panel Message

None

Possible Cause(s)

There is an error in the header of an MPEG packet.

Check and Correct

- 1 Check the upstream devices that are sending MPEG packets to the input ports on the Netcrypt.
- 2 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 3 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 4 If the alarm continues to occur, contact Cisco Services for further assistance.

Netcrypt Alarm ID 5 (5 Hex)

The Netcrypt **Input 3 MPEG Continuity Error** minor alarm occurs when individual MPEG packets become corrupted due to random noise in the network. Each MPEG packet has a section for continuity bits that should contain a sequential value. These MPEG continuity bits are used by the MPEG packet recipient to verify that the packets in an MPEG stream are received in the correct sequential order and to verify that no packet loss has occurred.

This alarm also occurs when the Netcrypt receives packets in the MPEG stream that do not contain MPEG continuity bits.

There is a potential for loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the Netcrypt that is sending this alarm.

Front Panel Message

None

Possible Cause(s)

- A cable is loose, disconnected, or defective.
- There are data errors on the satellite link.
- The rate of change of the IEC exceeds the allowed threshold.
- There is defective upstream equipment or failure on the input data link of the Netcrypt.
- There is defective local MPEG coding.
- The Netcrypt is defective.

Check and Correct

Loose, disconnected, or defective cables

Check for loose connections or defective cables, tighten any loose cable connections, connect any disconnected cables, and replace any defective cables.

Satellite link data errors

Contact your signal provider to verify if there are any problems with their satellite transmissions.

IEC errors

Clean up the MPEG signal input to the Netcrypt by checking the IRT, RTE, and MPEG encoder along with the GigE stream.

Chapter 4 Netcrypt Alarms

Defective upstream equipment

- 1 Check the upstream devices that are sending MPEG packets to the Netcrypt.
- 2 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of service.

Important!

- If the majority of MPEG packet alarms are occurring in a single Netcrypt, then that Netcrypt or its input should be the focus of the troubleshooting.
 - If the majority of MPEG packet alarms are occurring in more than one Netcrypt, then the troubleshooting should focus upstream on the device that is providing a common source of input to the Netcrypt with errors.
 - If the Netcrypt has a common device upstream, then that device is the most likely source of the packet errors
- 3 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
 - 4 If the alarm continues to occur, contact Cisco Services for further assistance.

Defective local MPEG coding

Check the local source devices that are providing MPEG content to the Netcrypt.

Netcrypt is defective

- 1 Replace the Netcrypt if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the Netcrypt.
- 2 If the alarm continues to occur, contact Cisco Services for further assistance.

Netcrypt Alarm ID 6 (6 Hex)

The Netcrypt **Input 3 MPEG Transport Error** minor alarm occurs when there is an error in the header of some of the MPEG packets received by the Netcrypt. There is a potential for loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the Netcrypt that is sending this alarm.

Note: This alarm is self-clearing and may be intermittent. Single instances of this alarm that clear automatically and that do not reappear are not a cause for concern.

Front Panel Message

None

Possible Cause(s)

There is an error in the header of an MPEG packet.

Check and Correct

- 1 Check the upstream devices that are sending MPEG packets to the input ports on the Netcrypt.
- 2 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 3 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 4 If the alarm continues to occur, contact Cisco Services for further assistance.

Netcrypt Alarm ID 7 (7 Hex)

The **Netcrypt Input 4 MPEG Continuity Error** minor alarm occurs when individual MPEG packets become corrupted due to random noise in the network. Each MPEG packet has a section for continuity bits that should contain a sequential value. These MPEG continuity bits are used by the MPEG packet recipient to verify that the packets in an MPEG stream are received in the correct sequential order and to verify that no packet loss has occurred.

This alarm also occurs when the Netcrypt receives packets in the MPEG stream that do not contain MPEG continuity bits.

There is a potential for loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the Netcrypt that is sending this alarm.

Front Panel Message

None

Possible Cause(s)

- A cable is loose, disconnected, or defective.
- There are data errors on the satellite link.
- The rate of change of the IEC exceeds the allowed threshold.
- There is defective upstream equipment or failure on the input data link of the Netcrypt.
- There is defective local MPEG coding.
- The Netcrypt is defective.

Check and Correct

Loose, disconnected, or defective cables

Check for loose connections or defective cables, tighten any loose cable connections, connect any disconnected cables, and replace any defective cables.

Satellite link data errors

Contact your signal provider to verify if there are any problems with their satellite transmissions.

IEC errors

Clean up the MPEG signal input to the Netcrypt by checking the IRT, RTE, and MPEG encoder along with the GigE stream.

Defective upstream equipment

- 1 Check the upstream devices that are sending MPEG packets to the Netcrypt.
- 2 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of service.

Important!

- If the majority of MPEG packet alarms are occurring in a single Netcrypt, then that Netcrypt or its input should be the focus of the troubleshooting.
 - If the majority of MPEG packet alarms are occurring in more than one Netcrypt, then the troubleshooting should focus upstream on the device that is providing a common source of input to the Netcrypt with errors.
 - If the Netcrypt has a common device upstream, then that device is the most likely source of the packet errors
- 3 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
 - 4 If the alarm continues to occur, contact Cisco Services for further assistance.

Defective local MPEG coding

Check the local source devices that are providing MPEG content to the Netcrypt.

Netcrypt is defective

- 1 Replace the Netcrypt if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the Netcrypt.
- 2 If the alarm continues to occur, contact Cisco Services for further assistance.

Netcrypt Alarm ID 8 (8 Hex)

The **Netcrypt Input 4 MPEG Transport Error** minor alarm occurs when there is an error in the header of some of the MPEG packets received by the Netcrypt. There is a potential for loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the Netcrypt that is sending this alarm.

Note: This alarm is self-clearing and may be intermittent. Single instances of this alarm that clear automatically and that do not reappear are not a cause for concern.

Front Panel Message

None

Possible Cause(s)

There is an error in the header of an MPEG packet.

Check and Correct

- 1 Check the upstream devices that are sending MPEG packets to the input ports on the Netcrypt.
- 2 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 3 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 4 If the alarm continues to occur, contact Cisco Services for further assistance.

Netcrypt Alarm ID 17 (11 Hex)

The **Netcrypt Input 1 Loss of Input Signal Synchronization** major alarm occurs when the Netcrypt could not lock onto a valid input MPEG2 stream at port 1 in the Netcrypt. Active program and data services that are present on port 1 are not available.

Important! If you receive the loss of signal synchronization alarm for an input that you are intentionally not using, you may ignore this alarm.

Front Panel Message

None

Possible Cause(s)

- A cable is loose, disconnected, or defective.
- An upstream device providing input to the Netcrypt failed or is offline.
- No sync byte found "value 0x47 hex"
- The Netcrypt is defective.

Check and Correct

A cable is loose, disconnected, or defective

Check for loose cable connections or defective cables at the inputs on the back panel of the Netcrypt, connect any disconnected cables, then tighten any loose cable connections, and replace any defective cables.

Upstream device failed or offline

- 1 Verify that the outputs of upstream devices are functioning correctly.
- 2 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 3 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 4 If the alarm continues to occur, contact Cisco Services for further assistance.

No sync byte found

Check the clock in the input stream.

Netcrypt is defective

- 1 Replace the Netcrypt if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the Netcrypt.
- 2 Contact Cisco Services for further assistance.

Netcrypt Alarm ID 18 (12 Hex)

The **Netcrypt Input 1 Errored MPEG Packet** minor alarm occurs when there are errors in the headers of the MPEG packets at port 1 in the Netcrypt. Errors include an invalid MPEG packet header where the first byte (for example, sync byte) is not equal to 47 Hex (0x47), or where the MPEG packet size is not exactly 188 bytes. There is a potential for loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the Netcrypt that is sending this alarm.

This alarm may also occur when the GigE cable is disconnected and then clear before you reconnect the cable. This alarm clear occurs because the MPEG stream is disrupted and the device detects that the input signal is completely lost.

Note: This alarm is self-clearing and may be intermittent. Single instances of this alarm that clear automatically and that do not reappear are not a cause for concern.

Front Panel Message

None

Possible Cause(s)

- A cable is loose, disconnected, or defective.
- There are data errors on the satellite link.
- The rate of change of the IEC exceeds the allowed threshold.
- Upstream devices that provide input to the Netcrypt are sending errored MPEG packets.
- There is defective local MPEG coding.
- The Netcrypt is defective.

Check and Correct

A cable is loose, disconnected, or defective

Check for loose connections or defective cables, tighten any loose cable connections, connect any disconnected cables, and replace any defective cables.

Note: This alarm may also occur when the GigE cable is disconnected and then clear before you reconnect the cable. This is normal.

Data errors on the satellite link

Contact your signal provider to verify if there are any problems with their satellite transmissions.

IEC exceeds threshold

Clean up the MPEG signal input to the Netcrypt by checking the IRT, RTE, and MPEG encoder along with the GigE connection.

Upstream devices sending errored MPEG packets

Check the upstream devices that are sending MPEG packets to port 1 in the Netcrypt.

Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.

Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.

If the alarm continues to occur, contact Cisco Services for further assistance.

Defective local MPEG coding

Check the local source devices that are providing MPEG content to the Netcrypt.

Netcrypt is defective

- 1** Replace the Netcrypt if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the Netcrypt.
- 2** Contact Cisco Services for further assistance.

Netcrypt Alarm ID 19 (13 Hex)

The **Netcrypt Input 1 FIFO Overflow** minor alarm occurs when there is a FIFO buffer overflow at port 1 on the Netcrypt, and packet data is lost. There is a potential for loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the Netcrypt that is sending this alarm.

Note: This alarm is self-clearing and may be intermittent. Single instances of this alarm that clear automatically and that do not reappear are not a cause for concern.

Front Panel Message

None

Possible Cause(s)

- The data rate as defined from the EC for the Netcrypt sessions is too low, which also means that the data rate of the GigE input to the Netcrypt is too high.
- There are too many sessions defined for the Netcrypt from the EC.
- Upstream devices are sending too many MPEG packets to the Netcrypt.
- A hardware problem occurred.

Check and Correct

Data rate too low

- 1 Reduce the amount of incoming data.
- 2 Reduce the amount of data added to the stream.
- 3 Verify and correct session rate targets and threshold values.

Too many sessions defined

Reduce the total number of MPEG programs by deleting sessions.

Upstream devices sending too many MPEG packets

Check the upstream devices that are sending MPEG packets to the input ports on the Netcrypt.

Hardware problem

- 1 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 2 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 3 Replace the Netcrypt if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the Netcrypt.
- 4 If the alarm continues to occur, contact Cisco Services for further assistance.

Netcrypt Alarm ID 20 (14 Hex)

The **Netcrypt Input 1 Packets Dumped** minor alarm occurs when there is excessive bandwidth utilization on one or more channels at port 1 on the Netcrypt. Packets for those channels are being dumped so as not to affect the other channels.

There is potential loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the Netcrypt that is sending this alarm.

Note: This alarm is self-clearing and may be intermittent. Single instances of this alarm that clear automatically and that do not reappear are not a cause for concern.

Front Panel Message

None

Possible Cause(s)

- The data rate as defined from the EC for the Netcrypt sessions is too low, which also means that the data rate of the input to the Netcrypt is too high.
- There are too many sessions defined for the Netcrypt from the EC.
- Upstream devices are sending too many MPEG packets to the Netcrypt.
- A hardware problem occurred.

Check and Correct

Data rate too low

- 1 Reduce the amount of incoming data.
- 2 Reduce the amount of data added to the stream.
- 3 Verify and correct session rate targets and threshold values.

Too many sessions defined

Reduce the total number of MPEG programs by deleting sessions.

Upstream devices sending too many MPEG packets

Check the upstream devices that are sending MPEG packets to the input ports on the Netcrypt.

Chapter 4 Netcrypt Alarms

Hardware problem

- 1 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 2 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 3 Replace the Netcrypt if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the Netcrypt.
- 4 If the alarm continues to occur, contact Cisco Services for further assistance.

Netcrypt Alarm ID 21 (15 Hex)

The **Netcrypt Input 2 Loss of Input Signal Synchronization** major alarm occurs when the Netcrypt could not lock onto a valid input MPEG2 stream at port 2 in the Netcrypt. Active program and data services that are present on port 2 are not available.

Important! If you receive the loss of signal synchronization alarm for an input that you are intentionally not using, you may ignore this alarm.

Front Panel Message

None

Possible Cause(s)

- A cable is loose, disconnected, or defective.
- An upstream device providing input to the Netcrypt failed or is offline.
- No sync byte found "value 0x47 hex.
- The Netcrypt is defective.

Check and Correct

A cable is loose, disconnected, or defective

Check for loose cable connections or defective cables at the inputs on the back panel of the Netcrypt, connect any disconnected cables, then tighten any loose cable connections, and replace any defective cables.

Upstream device failed or offline

- 1 Verify that the outputs of upstream devices are functioning correctly.
- 2 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 3 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 4 If the alarm continues to occur, contact Cisco Services for further assistance.

No sync byte found

Check the clock in the input stream.

Netcrypt is defective

- 1 Replace the Netcrypt if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the Netcrypt.
- 2 Contact Cisco Services for further assistance.

Netcrypt Alarm ID 22 (16 Hex)

The **Netcrypt Input 2 Errored MPEG Packet** minor alarm occurs when there are errors in the headers of the MPEG packets at port 2 in the Netcrypt. Errors include an invalid MPEG packet header where the first byte (for example, sync byte) is not equal to 47 Hex (0x47), or where the MPEG packet size is not exactly 188 bytes. There is a potential for loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the Netcrypt that is sending this alarm.

This alarm may also occur when the GigE cable is disconnected and then clear before you reconnect the cable. This alarm clear occurs because the MPEG stream is disrupted and the device detects that the input signal is completely lost.

Note: This alarm is self-clearing and may be intermittent. Single instances of this alarm that clear automatically and that do not reappear are not a cause for concern.

Front Panel Message

None

Possible Cause(s)

- A cable is loose, disconnected, or defective.
- There are data errors on the satellite link.
- The rate of change of the IEC exceeds the allowed threshold.
- Upstream devices that provide input to the Netcrypt are sending errored MPEG packets.
- There is defective local MPEG coding.
- The Netcrypt is defective.

Check and Correct

A cable is loose, disconnected, or defective

Check for loose connections or defective cables, tighten any loose cable connections, connect any disconnected cables, and replace any defective cables.

Note: This alarm may also occur when the cable is disconnected and then clear before you reconnect the cable. This is normal.

Data errors on the satellite link

Contact your signal provider to verify if there are any problems with their satellite transmissions.

IEC exceeds threshold

Clean up the MPEG signal input to the Netcrypt by checking the IRT, RTE, and MPEG encoder along with the GigE connection.

Upstream devices sending errored MPEG packets

- 1 Check the upstream devices that are sending MPEG packets to port 2 on the Netcrypt.
- 2 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 3 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 4 If the alarm continues to occur, contact Cisco Services for further assistance.

Defective local MPEG coding

Check the local source devices that are providing MPEG content to the Netcrypt.

Netcrypt is defective

- 1 Replace the Netcrypt if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the Netcrypt.
- 2 Contact Cisco Services for further assistance.

Netcrypt Alarm ID 23 (17 Hex)

The **Netcrypt Input 2 FIFO Overflow** minor alarm occurs when there is a FIFO buffer overflow at port 2 on the Netcrypt, and packet data is lost. There is a potential for loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the Netcrypt that is sending this alarm.

Note: This alarm is self-clearing and may be intermittent. Single instances of this alarm that clear automatically and that do not reappear are not a cause for concern.

Front Panel Message

None

Possible Cause(s)

- The data rate as defined from the EC for the Netcrypt sessions is too low, which also means that the data rate of the input to the Netcrypt is too high.
- There are too many sessions defined for the Netcrypt from the EC.
- Upstream devices are sending too many MPEG packets to the Netcrypt.
- A hardware problem occurred.

Check and Correct

Data rate too low

- 1 Reduce the amount of incoming data.
- 2 Reduce the amount of data added to the stream.
- 3 Verify and correct session rate targets and threshold values.

Too many sessions defined

Reduce the total number of MPEG programs by deleting sessions.

Upstream devices sending too many MPEG packets

Check the upstream devices that are sending MPEG packets to the input ports on the Netcrypt.

Hardware problem

- 1 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 2 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 3 Replace the Netcrypt if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the Netcrypt.
- 4 If the alarm continues to occur, contact Cisco Services for further assistance.

Netcrypt Alarm ID 24 (18 Hex)

The **Netcrypt Input 2 Packets Dumped** minor alarm occurs when there is excessive bandwidth utilization on one or more channels at port 2 on the Netcrypt. Packets for those channels are being dumped so as not to affect the other channels.

There is potential loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the Netcrypt that is sending this alarm.

Note: This alarm is self-clearing and may be intermittent. Single instances of this alarm that clear automatically and that do not reappear are not a cause for concern.

Front Panel Message

None

Possible Cause(s)

The data rate as defined from the EC for the Netcrypt sessions is too low, which also means that the data rate of the input to the Netcrypt is too high.

There are too many sessions defined for the Netcrypt from the EC.

Upstream devices are sending too many MPEG packets to the Netcrypt.

A hardware problem occurred.

Check and Correct

Data rate too low

- 1 Reduce the amount of incoming data.
- 2 Reduce the amount of data added to the stream.
- 3 Verify and correct session rate targets and threshold values.

Too many sessions defined

Reduce the total number of MPEG programs by deleting sessions.

Upstream devices sending too many MPEG packets

Check the upstream devices that are sending MPEG packets to the input ports on the Netcrypt.

Chapter 4 Netcrypt Alarms

Hardware problem

- 1 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 2 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 3 Replace the Netcrypt if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the Netcrypt.
- 4 If the alarm continues to occur, contact Cisco Services for further assistance.

Netcrypt Alarm ID 25 (19 Hex)

The **Netcrypt Input 3 Loss of Input Signal Synchronization** major alarm occurs when the Netcrypt could not lock onto a valid input MPEG2 stream at port 3 in the Netcrypt. Active program and data services that are present on port 3 are not available.

Important! If you receive the loss of signal synchronization alarm for an input that you are intentionally not using, you may ignore this alarm.

Front Panel Message

None

Possible Cause(s)

- A cable is loose, disconnected, or defective.
- An upstream device providing input to the Netcrypt failed or is offline.
- No sync byte found "value 0x47 hex."
- The Netcrypt is defective.

Check and Correct

A cable is loose, disconnected, or defective

Check for loose cable connections or defective cables at the inputs on the back panel of the Netcrypt, connect any disconnected cables, then tighten any loose cable connections, and replace any defective cables.

Upstream device failed or offline

- 1 Verify that the outputs of upstream devices are functioning correctly.
- 2 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 3 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 4 If the alarm continues to occur, contact Cisco Services for further assistance.

No sync byte found

Check the clock in the input stream.

Netcrypt is defective

- 1 Replace the Netcrypt if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the Netcrypt.
- 2 Contact Cisco Services for further assistance.

Netcrypt Alarm ID 26 (1A Hex)

The **Netcrypt Input 3 Errored MPEG Packet** minor alarm occurs when there are errors in the headers of the MPEG packets at port 3 in the Netcrypt. Errors include an invalid MPEG packet header where the first byte (for example, sync byte) is not equal to 47 Hex (0x47), or where the MPEG packet size is not exactly 188 bytes. There is a potential for loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the Netcrypt that is sending this alarm.

This alarm may also occur when the GigE cable is disconnected and then clear before you reconnect the cable. This alarm clear occurs because the MPEG stream is disrupted and the device detects that the input signal is completely lost.

Note: This alarm is self-clearing and may be intermittent. Single instances of this alarm that clear automatically and that do not reappear are not a cause for concern.

Front Panel Message

None

Possible Cause(s)

- A cable is loose, disconnected, or defective.
- There are data errors on the satellite link.
- The rate of change of the IEC exceeds the allowed threshold.
- Upstream devices that provide input to the Netcrypt are sending errored MPEG packets.
- There is defective local MPEG coding.
- The Netcrypt is defective.

Check and Correct

A cable is loose, disconnected, or defective

Check for loose connections or defective cables, tighten any loose cable connections, connect any disconnected cables, and replace any defective cables.

Note: This alarm may also occur when the cable is disconnected and then clear before you reconnect the cable. This is normal.

Data errors on the satellite link

Contact your signal provider to verify if there are any problems with their satellite transmissions.

IEC exceeds threshold

Clean up the MPEG signal input to the Netcrypt by checking the IRT, RTE, and MPEG encoder along with the GigE connection.

Upstream devices sending errored MPEG packets

- 1 Check the upstream devices that are sending MPEG packets to port 3 on the Netcrypt.
- 2 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 3 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 4 If the alarm continues to occur, contact Cisco Services for further assistance.

Defective local MPEG coding

Check the local source devices that are providing MPEG content to the Netcrypt.

Netcrypt is defective

- 1 Replace the Netcrypt if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the Netcrypt.
- 2 Contact Cisco Services for further assistance.

Netcrypt Alarm ID 27 (1B Hex)

The **Netcrypt Input 3 FIFO Overflow** minor alarm occurs when there is a FIFO buffer overflow at port 3 on the Netcrypt, and packet data is lost. There is a potential for loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the Netcrypt that is sending this alarm.

Note: This alarm is self-clearing and may be intermittent. Single instances of this alarm that clear automatically and that do not reappear are not a cause for concern.

Front Panel Message

None

Possible Cause(s)

The data rate as defined from the EC for the Netcrypt sessions is too low, which also means that the data rate of the input to the Netcrypt is too high.

There are too many sessions defined for the Netcrypt from the EC.

Upstream devices are sending too many MPEG packets to the Netcrypt.

A hardware problem occurred.

Check and Correct

Data rate too low

- 1 Reduce the amount of incoming data.
- 2 Reduce the amount of data added to the stream.
- 3 Verify and correct session rate targets and threshold values.

Too many sessions defined

Reduce the total number of MPEG programs by deleting sessions.

Upstream devices sending too many MPEG packets

Check the upstream devices that are sending MPEG packets to the input ports on the Netcrypt.

Hardware problem

- 1 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 2 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 3 Replace the Netcrypt if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the Netcrypt.
- 4 If the alarm continues to occur, contact Cisco Services for further assistance.

Netcrypt Alarm ID 28 (1C Hex)

The **Netcrypt Input 3 Packets Dumped** minor alarm occurs when there is excessive bandwidth utilization on one or more channels at port 3 on the Netcrypt. Packets for those channels are being dumped so as not to affect the other channels.

There is potential loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the Netcrypt that is sending this alarm.

Note: This alarm is self-clearing and may be intermittent. Single instances of this alarm that clear automatically and that do not reappear are not a cause for concern.

Front Panel Message

None

Possible Cause(s)

- The data rate as defined from the EC for the Netcrypt sessions is too low, which also means that the data rate of the input to the Netcrypt is too high.
- There are too many sessions defined for the Netcrypt from the EC.
- Upstream devices are sending too many MPEG packets to the Netcrypt.
- A hardware problem occurred.

Check and Correct

Data rate too low

- 1 Reduce the amount of incoming data.
- 2 Reduce the amount of data added to the stream.
- 3 Verify and correct session rate targets and threshold values.

Too many sessions defined

Reduce the total number of MPEG programs by deleting sessions.

Upstream devices sending too many MPEG packets

Check the upstream devices that are sending MPEG packets to the input ports on the Netcrypt.

Chapter 4 Netcrypt Alarms

Hardware problem

- 1 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 2 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 3 Replace the Netcrypt if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the Netcrypt.
- 4 If the alarm continues to occur, contact Cisco Services for further assistance.

Netcrypt Alarm ID 29 (1D Hex)

The **Netcrypt Input 4 Loss of Input Signal Synchronization** major alarm occurs when the Netcrypt could not lock onto a valid input MPEG2 stream at port 4 in the Netcrypt. Active program and data services that are present on port 4 are not available.

Important! If you receive the loss of signal synchronization alarm for an input that you are intentionally not using, you may ignore this alarm.

Front Panel Message

None

Possible Cause(s)

- A cable is loose, disconnected, or defective.
- An upstream device providing input to the Netcrypt failed or is offline.
- No sync byte found "value 0x47 hex"
- The Netcrypt is defective.

Check and Correct

A cable is loose, disconnected, or defective

Check for loose cable connections or defective cables at the inputs on the back panel of the Netcrypt, connect any disconnected cables, then tighten any loose cable connections, and replace any defective cables.

Upstream device failed or offline

- 1 Verify that the outputs of upstream devices are functioning correctly.
- 2 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 3 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 4 If the alarm continues to occur, contact Cisco Services for further assistance.

No sync byte found

Check the clock in the input stream.

Netcrypt is defective

- 1 Replace the Netcrypt if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the Netcrypt.
- 2 Contact Cisco Services for further assistance.

Netcrypt Alarm ID 30 (1D Hex)

The **Netcrypt Input 4 Errored MPEG Packet** minor alarm occurs when there are errors in the headers of the MPEG packets at port 4 in the Netcrypt. Errors include an invalid MPEG packet header where the first byte (for example, sync byte) is not equal to 47 Hex (0x47), or where the MPEG packet size is not exactly 188 bytes. There is a potential for loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the Netcrypt that is sending this alarm.

This alarm may also occur when the GigE cable is disconnected and then clear before you reconnect the cable. This alarm clear occurs because the MPEG stream is disrupted and the device detects that the input signal is completely lost.

Note: This alarm is self-clearing and may be intermittent. Single instances of this alarm that clear automatically and that do not reappear are not a cause for concern.

Front Panel Message

None

Possible Cause(s)

- A cable is loose, disconnected, or defective.
- There are data errors on the satellite link.
- The rate of change of the IEC exceeds the allowed threshold.
- Upstream devices that provide input to the Netcrypt are sending errored MPEG packets.
- There is defective local MPEG coding.
- The Netcrypt is defective.

Check and Correct

A cable is loose, disconnected, or defective

Check for loose connections or defective cables, tighten any loose cable connections, connect any disconnected cables, and replace any defective cables.

Note: This alarm may also occur when the cable is disconnected and then clear before you reconnect the cable. This is normal.

Data errors on the satellite link

Contact your signal provider to verify if there are any problems with their satellite transmissions.

IEC exceeds threshold

Clean up the MPEG signal input to the Netcrypt by checking the , IRT, RTE, and MPEG encoder along with the GigE connection.

Upstream devices sending errored MPEG packets

- 1 Check the upstream devices that are sending MPEG packets to port 4 on the Netcrypt.
- 2 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 3 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 4 If the alarm continues to occur, contact Cisco Services for further assistance.

Defective local MPEG coding

Check the local source devices that are providing MPEG content to the Netcrypt.

Netcrypt is defective

- 1 Replace the Netcrypt if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the Netcrypt.
- 2 Contact Cisco Services for further assistance.

Netcrypt Alarm ID 31 (1F Hex)

The **Netcrypt Input 4 FIFO Overflow** minor alarm occurs when there is a FIFO buffer overflow at port 4 on the Netcrypt, and packet data is lost. There is a potential for loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the Netcrypt that is sending this alarm.

Note: This alarm is self-clearing and may be intermittent. Single instances of this alarm that clear automatically and that do not reappear are not a cause for concern.

Front Panel Message

None

Possible Cause(s)

- The data rate as defined from the EC for the Netcrypt sessions is too low, which also means that the data rate of the input to the Netcrypt is too high.
- There are too many sessions defined for the Netcrypt from the EC.
- Upstream devices are sending too many MPEG packets to the Netcrypt.
- A hardware problem occurred.

Check and Correct

Data rate too low

- 1 Reduce the amount of incoming data.
- 2 Reduce the amount of data added to the stream.
- 3 Verify and correct session rate targets and threshold values.

Too many sessions defined

Reduce the total number of MPEG programs by deleting sessions.

Upstream devices sending too many MPEG packets

Check the upstream devices that are sending MPEG packets to the input ports on the Netcrypt.

Hardware problem

- 1 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 2 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 3 Replace the Netcrypt if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the Netcrypt.
- 4 If the alarm continues to occur, contact Cisco Services for further assistance.

Netcrypt Alarm ID 32 (20 Hex)

The **Netcrypt Input 4 Packets Dumped** minor alarm occurs when there is excessive bandwidth utilization on one or more channels at port 4 on the Netcrypt. Packets for those channels are being dumped so as not to affect the other channels.

There is potential loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the Netcrypt that is sending this alarm.

Note: This alarm is self-clearing and may be intermittent. Single instances of this alarm that clear automatically and that do not reappear are not a cause for concern.

Front Panel Message

None

Possible Cause(s)

- The data rate as defined from the EC for the Netcrypt sessions is too low, which also means that the data rate of the input to the Netcrypt is too high.
- There are too many sessions defined for the Netcrypt from the EC.
- Upstream devices are sending too many MPEG packets to the Netcrypt.
- A hardware problem occurred.

Check and Correct

Data rate too low

- 1 Reduce the amount of incoming data.
- 2 Reduce the amount of data added to the stream.
- 3 Verify and correct session rate targets and threshold values.

Too many sessions defined

Reduce the total number of MPEG programs by deleting sessions.

Upstream devices sending too many MPEG packets

Check the upstream devices that are sending MPEG packets to the input ports on the Netcrypt.

Chapter 4 Netcrypt Alarms

Hardware problem

- 1 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 2 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 3 Replace the Netcrypt if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the Netcrypt.
- 4 If the alarm continues to occur, contact Cisco Services for further assistance.

Netcrypt Alarm ID 49 (31 Hex)

The **Netcrypt Ethernet 1 Loss of Signal** minor alarm occurs when there is no signal to port 1 in the Netcrypt. Active program and data services that are present on port 1 are not available.

Important! If you receive the loss of signal alarm an input that you are intentionally not using, you may ignore this alarm.

Front Panel Message

None

Possible Cause(s)

- A cable is loose, disconnected, or defective.
- An upstream device providing input to the Netcrypt failed or is offline.
- The Netcrypt is defective.

Check and Correct

A cable is loose, disconnected, or defective

Check for loose cable connections or defective cables at the inputs on the back panel of the Netcrypt, connect any disconnected cables, then tighten any loose cable connections, and replace any defective cables.

Upstream device failed or offline

- 1 Verify that the outputs of upstream devices are functioning correctly.
- 2 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 3 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 4 If the alarm continues to occur, contact Cisco Services for further assistance.

Netcrypt is defective

- 1 Replace the Netcrypt if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the Netcrypt.
- 2 Contact Cisco Services for further assistance.

Netcrypt Alarm ID 50 (32 Hex)

The **Netcrypt Ethernet 2 Loss of Signal** minor alarm occurs when there is no signal to port 2 in the Netcrypt. Active program and data services that are present on port 2 are not available.

Important! If you receive the loss of signal alarm an input that you are intentionally not using, you may ignore this alarm.

Front Panel Message

None

Possible Cause(s)

- A cable is loose, disconnected, or defective.
- An upstream device providing input to the Netcrypt failed or is offline.
- The Netcrypt is defective.

Check and Correct

A cable is loose, disconnected, or defective

Check for loose cable connections or defective cables at the inputs on the back panel of the Netcrypt, connect any disconnected cables, then tighten any loose cable connections, and replace any defective cables.

Upstream device failed or offline

- 1 Verify that the outputs of upstream devices are functioning correctly.
- 2 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 3 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 4 If the alarm continues to occur, contact Cisco Services for further assistance.

Netcrypt is defective

- 1 Replace the Netcrypt if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the Netcrypt.
- 2 Contact Cisco Services for further assistance.

Netcrypt Alarm ID 51 (33 Hex)

The **Netcrypt Ethernet 3 Loss of Signal** minor alarm occurs when there is no signal to port 3 in the Netcrypt. Active program and data services that are present on port 3 are not available.

Important! If you receive the loss of signal alarm an input that you are intentionally not using, you may ignore this alarm.

Front Panel Message

None

Possible Cause(s)

- A cable is loose, disconnected, or defective.
- An upstream device providing input to the Netcrypt failed or is offline.
- The Netcrypt is defective.

Check and Correct

A cable is loose, disconnected, or defective

Check for loose cable connections or defective cables at the inputs on the back panel of the Netcrypt, connect any disconnected cables, then tighten any loose cable connections, and replace any defective cables.

Upstream device failed or offline

- 1 Verify that the outputs of upstream devices are functioning correctly.
- 2 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 3 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 4 If the alarm continues to occur, contact Cisco Services for further assistance.

Netcrypt is defective

- 1 Replace the Netcrypt if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the Netcrypt.
- 2 Contact Cisco Services for further assistance.

Netcrypt Alarm ID 52 (34 Hex)

The **Netcrypt Ethernet 4 Loss of Signal** minor alarm occurs when there is no signal to port 4 in the Netcrypt. Active program and data services that are present on port 4 are not available.

Important! If you receive the loss of signal alarm an input that you are intentionally not using, you may ignore this alarm.

Front Panel Message

None

Possible Cause(s)

- A cable is loose, disconnected, or defective.
- An upstream device providing input to the Netcrypt failed or is offline.
- The Netcrypt is defective.

Check and Correct

A cable is loose, disconnected, or defective

Check for loose cable connections or defective cables at the inputs on the back panel of the Netcrypt, connect any disconnected cables, then tighten any loose cable connections, and replace any defective cables.

Upstream device failed or offline

- 1 Verify that the outputs of upstream devices are functioning correctly.
- 2 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 3 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 4 If the alarm continues to occur, contact Cisco Services for further assistance.

Netcrypt is defective

- 1 Replace the Netcrypt if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the Netcrypt.
- 2 Contact Cisco Services for further assistance.

Netcrypt Alarm ID 57 (39 Hex)

The **Netcrypt Output 1 FIFO Overflow** minor alarm occurs when there is a FIFO overflow at output Channel 1 on the Netcrypt, and packet data is lost. There is a low potential for loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the Netcrypt that is sending this alarm.

Note: This alarm is self-clearing and may be intermittent. Single instances of this alarm that clear automatically and that do not reappear are not a cause for concern.

Front Panel Message

None

Possible Cause(s)

- The data rate as defined from the EC for the Netcrypt sessions is too low, which also means that the data rate of the input to the Netcrypt is too high.
- There are too many sessions defined for the Netcrypt from the EC.
- A hardware problem occurred.

Check and Correct

Data rate is too low

- 1 Reduce the amount of incoming data.
- 2 Reduce the amount of data added to the stream.
- 3 Verify and correct session rate targets and threshold values.

Too many sessions defined

Reduce the total number of MPEG programs by deleting sessions.

Hardware problem

- 1 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 2 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 3 If the alarm continues to occur, contact Cisco Services for further assistance.

Netcrypt Alarm ID 58 (3A Hex)

The **Netcrypt Output 1 Packets Dumped** minor alarm occurs when the Netcrypt is dropping low priority packets at output Channel 1. Low priority packets are being dropped because the number of packets at output Channel 1 exceeds its capacity.

Note: This alarm is self-clearing and may be intermittent. Single instances of this alarm that clear automatically and that do not reappear are not a cause for concern.

There is a low potential for loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the Netcrypt that is sending this alarm.

Front Panel Message

None

Possible Cause(s)

- The data rate as defined from the EC for the Netcrypt sessions is too low, which also means that the data rate of the input to the Netcrypt is too high.
- There are too many sessions defined for the Netcrypt from the EC.
- A hardware problem occurred.

Check and Correct

Data rate is too low

- 1 Reduce the amount of incoming data.
- 2 Reduce the amount of data added to the stream.
- 3 Verify and correct session rate targets and threshold values.

Too many sessions defined

Reduce the total number of MPEG programs by deleting sessions.

Hardware problem

- 1 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 2 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 3 Replace the Netcrypt if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the Netcrypt.
- 4 If the alarm continues to occur, contact Cisco Services for further assistance.

Netcrypt Alarm ID 59 (3B Hex)

The **Netcrypt Output 2 FIFO Overflow** minor alarm occurs when there is a FIFO overflow at output Channel 2 on the Netcrypt, and packet data is lost. There is a low potential for loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the Netcrypt that is sending this alarm.

Note: This alarm is self-clearing and may be intermittent. Single instances of this alarm that clear automatically and that do not reappear are not a cause for concern.

Front Panel Message

None

Possible Cause(s)

- The data rate as defined from the EC for the Netcrypt sessions is too low, which also means that the data rate of the input to the Netcrypt is too high.
- There are too many sessions defined for the Netcrypt from the EC.
- A hardware problem occurred.

Check and Correct

Data rate is too low

- 1 Reduce the amount of incoming data.
- 2 Reduce the amount of data added to the stream.
- 3 Verify and correct session rate targets and threshold values.

Too many sessions defined

Reduce the total number of MPEG programs by deleting sessions.

Hardware problem

- 1 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 2 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 3 If the alarm continues to occur, contact Cisco Services for further assistance.

Netcrypt Alarm ID 60 (3C Hex)

The **Netcrypt Output 2 Packets Dumped** minor alarm occurs when the Netcrypt is dropping low priority packets at output Channel 2. Low priority packets are being dropped because the number of packets at output Channel 2 exceeds its capacity.

Note: This alarm is self-clearing and may be intermittent. Single instances of this alarm that clear automatically and that do not reappear are not a cause for concern.

There is a low potential for loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the Netcrypt that is sending this alarm.

Front Panel Message

None

Possible Cause(s)

- The data rate as defined from the EC for the Netcrypt sessions is too low, which also means that the data rate of the input to the Netcrypt is too high.
- There are too many sessions defined for the Netcrypt from the EC.
- A hardware problem occurred.

Check and Correct

Data rate is too low

- 1 Reduce the amount of incoming data.
- 2 Reduce the amount of data added to the stream.
- 3 Verify and correct session rate targets and threshold values.

Too many sessions defined

Reduce the total number of MPEG programs by deleting sessions.

Hardware problem

- 1 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 2 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 3 Replace the Netcrypt if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the Netcrypt.
- 4 If the alarm continues to occur, contact Cisco Services for further assistance.

Netcrypt Alarm ID 61 (3D Hex)

The **Netcrypt Output 3 FIFO Overflow** minor alarm occurs when there is a FIFO overflow at output Channel 3 on the Netcrypt, and packet data is lost. There is a low potential for loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the Netcrypt that is sending this alarm.

Note: This alarm is self-clearing and may be intermittent. Single instances of this alarm that clear automatically and that do not reappear are not a cause for concern.

Front Panel Message

None

Possible Cause(s)

- The data rate as defined from the EC for the Netcrypt sessions is too low, which also means that the data rate of the input to the Netcrypt is too high.
- There are too many sessions defined for the Netcrypt from the EC.
- A hardware problem occurred.

Check and Correct

Data rate is too low

- 1 Reduce the amount of incoming data.
- 2 Reduce the amount of data added to the stream.
- 3 Verify and correct session rate targets and threshold values.

Too many sessions defined

Reduce the total number of MPEG programs by deleting sessions.

Hardware problem

- 1 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 2 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 3 If th alarm continues to occur, contact Cisco Services for further assistance.

Netcrypt Alarm ID 62 (3E Hex)

The **Netcrypt Output 3 Packets Dumped** minor alarm occurs when the Netcrypt is dropping low priority packets at output Channel 3. Low priority packets are being dropped because the number of packets at output Channel 3 exceeds its capacity.

Note: This alarm is self-clearing and may be intermittent. Single instances of this alarm that clear automatically and that do not reappear are not a cause for concern.

There is a low potential for loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the Netcrypt that is sending this alarm.

Front Panel Message

None

Possible Cause(s)

- The data rate as defined from the EC for the Netcrypt sessions is too low, which also means that the data rate of the input to the Netcrypt is too high.
- There are too many sessions defined for the Netcrypt from the EC.
- A hardware problem occurred.

Check and Correct

Data rate is too low

- 1 Reduce the amount of incoming data.
- 2 Reduce the amount of data added to the stream.
- 3 Verify and correct session rate targets and threshold values.

Too many sessions defined

Reduce the total number of MPEG programs by deleting sessions.

Hardware problem

- 1 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 2 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 3 Replace the Netcrypt if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the Netcrypt.
- 4 If the alarm continues to occur, contact Cisco Services for further assistance.

Netcrypt Alarm ID 63 (3F Hex)

The **Netcrypt Output 4 FIFO Overflow** minor alarm occurs when there is a FIFO overflow at output Channel 4 on the Netcrypt, and packet data is lost. There is a low potential for loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the Netcrypt that is sending this alarm.

Note: This alarm is self-clearing and may be intermittent. Single instances of this alarm that clear automatically and that do not reappear are not a cause for concern.

Front Panel Message

None

Possible Cause(s)

- The data rate as defined from the EC for the Netcrypt sessions is too low, which also means that the data rate of the input to the Netcrypt is too high.
- There are too many sessions defined for the Netcrypt from the EC.
- A hardware problem occurred.

Check and Correct

Data rate is too low

- 1 Reduce the amount of incoming data.
- 2 Reduce the amount of data added to the stream.
- 3 Verify and correct session rate targets and threshold values.

Too many sessions defined

Reduce the total number of MPEG programs by deleting sessions.

Hardware problem

- 1 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 2 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 3 If the alarm continues to occur, contact Cisco Services for further assistance.

Netcrypt Alarm ID 64 (40 Hex)

The **Netcrypt Output 4 Packets Dumped** minor alarm occurs when the Netcrypt is dropping low priority packets at output Channel 4. Low priority packets are being dropped because the number of packets at output Channel 4 exceeds its capacity.

Note: This alarm is self-clearing and may be intermittent. Single instances of this alarm that clear automatically and that do not reappear are not a cause for concern.

There is a low potential for loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the Netcrypt that is sending this alarm.

Front Panel Message

None

Possible Cause(s)

- The data rate as defined from the EC for the Netcrypt sessions is too low, which also means that the data rate of the input to the Netcrypt is too high.
- There are too many sessions defined for the Netcrypt from the EC.
- A hardware problem occurred.

Check and Correct

Data rate is too low

- 1 Reduce the amount of incoming data.
- 2 Reduce the amount of data added to the stream.
- 3 Verify and correct session rate targets and threshold values.

Too many sessions defined

Reduce the total number of MPEG programs by deleting sessions.

Hardware problem

- 1 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 2 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 3 Replace the Netcrypt if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the Netcrypt.
- 4 If the alarm continues to occur, contact Cisco Services for further assistance.

Netcrypt Alarm ID 73 (49 Hex)

The Netcrypt **Reset Detected** status alarm occurs during the boot-up process or when the Netcrypt is reset by either a loss of power or a manual reset. There is a potential for loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the Netcrypt that is sending this event until it returns for full service.

Front Panel Message

None

Possible Cause(s)

- The Netcrypt is rebooting.
- A user or system operator reset the Netcrypt.
- A loss of power occurred.
- There is a problem in the DBDS.

Check and Correct

Session and provisioning data are sent to the Netcrypt again by the EC. However, you should also check the following:

- 1 Verify that there are still broadcast services on the Netcrypt .
- 2 Verify that the reset did not adversely affect broadcast services.
- 3 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 4 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 5 Contact Cisco Services for further assistance.

Netcrypt Alarm ID 74 (4A Hex)

The Netcrypt **General Purpose Hardware error** major alarm occurs when there is a hardware failure in the Netcrypt. When this condition exists, there is a potential for loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the Netcrypt that is sending this alarm.

Front Panel Message

None

Possible Cause(s)

A hardware failure occurred.

Check and Correct

- 1 Power down and then power up the Netcrypt using the on/off rocker-type switch on the back panel, or reset the Netcrypt from the EC.
- 2 Replace the Netcrypt if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the Netcrypt.
- 3 If the alarm continues to occur, contact Cisco Services for further assistance.

Netcrypt Alarm ID 75 (4B Hex)

The Netcrypt **General Purpose Software Error** (runtime) major alarm displays when low-level software errors occur in the Netcrypt. When this condition exists, there is a potential for loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the Netcrypt that is sending this alarm.

Front Panel Message

None

Possible Cause(s)

Low-level software errors occurred.

Check and Correct

- 1 If this alarm continues to occur, power down and then power up the Netcrypt using the on/off rocker-type switch on the back panel, or reset the Netcrypt from the EC.
- 2 If resetting the Netcrypt does not solve the problem, contact Cisco Services for further assistance.

Netcrypt Alarm ID 76 (4C Hex)

The Netcrypt **Craft Port Event Change** status event occurs when a user or a system operator uses the craft port to view or change the settings on the Netcrypt. There is a potential for loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the Netcrypt that is sending this event.

Front Panel Message

None

Possible Cause(s)

A user or a system operator viewed or changed the settings on the Netcrypt from the craft port.

Check and Correct

- 1 Check to see if any settings were changed.
- 2 Are all services functioning correctly?
 - If **yes**, no further action is required.
 - If **no**, go to step 3.
- 3 Restore the settings to the previous configuration.
- 4 Power down and then power up the Netcrypt using the on/off rocker-type switch on the back panel, or reset the Netcrypt from the EC to restore the previous configuration.
- 5 If resetting the Netcrypt does not solve the problem, contact Cisco Services for further assistance.

Netcrypt Alarm ID 78 (4E Hex)

The Netcrypt **Third-Party CA Parameters Not Provisioned** minor alarm occurs when the Netcrypt does not receive the *qprovisionThirdPartyCaResponse* CA message from the EC. The Netcrypt will not attempt to connect to external devices such as the EIS and the ECMG while this alarm is active. There is a potential for loss of programming content relative to the Netcrypt that is sending this alarm.

Front Panel Message

None

Possible Cause(s)

The Netcrypt failed to connect to the EC qamManager process.

Check and Correct

- 1 Check for loose connections or defective cables, tighten any loose cable connections, connect any disconnected cables, and replace any defective cables.
- 2 Verify that the qamManager process on the EC is running.
- 3 If the alarm continues to occur, contact Cisco Services for further assistance.

Netcrypt Alarm ID 79 (4F Hex)

The Netcrypt **CA EIS Link Lost** minor alarm occurs when the TCP/IP link has not been established with the Primary EIS. This alarm will only be sent again one time if the TCP/IP link is established with the Primary EIS and then subsequently fails.

There is a potential for loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the Netcrypt that is sending this alarm. This alarm also indicates that the signal is being transmitted in the clear, when it should be encrypted.

Note: The Netcrypt will continually attempt to establish a TCP/IP link and communication with the Primary EIS until a TCP/IP link and communication is established. When a communication link is established, if any EIS link/connection alarms are active, the Netcrypt clears those alarms.

Front Panel Message

None

Possible Cause(s)

Cables are loose, disconnected, or defective.

The EIS is not operational.

Check and Correct

- 1 Check for loose connections or defective cables, tighten any loose cable connections, connect any disconnected cables, and replace any defective cables.
- 2 Verify that the EIS is operating correctly.
- 3 If the alarm continues to occur, contact Cisco Services for further assistance.

Netcrypt Alarm ID 80 (50 Hex)

The Netcrypt **Application Layer Connection to EIS Failed** minor alarm occurs when the TCP/IP link is established, but the Netcrypt is not communicating with the Primary EIS. This alarm remains active until the Primary EIS establishes communication at which time the Netcrypt clears the alarm. There is a potential for loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the Netcrypt that is sending this alarm. This alarm also indicates that the signal is being transmitted in the clear, when it should be encrypted.

Note: This alarm will only be sent again one time if the Primary EIS establishes communication and subsequently fails.

Front Panel Message

None

Possible Cause(s)

Cables are loose, disconnected, or defective.

The EIS connection parameters in the EC are not correct.

Check and Correct

- 1 Check for loose connections or defective cables, tighten any loose cable connections, connect any disconnected cables, and replace any defective cables.
- 2 Check and verify the EIS connection parameters in the EC.
- 3 If the alarm continues to occur, contact Cisco Services for further assistance.

Netcrypt Alarm ID 81 (51 Hex)

The Netcrypt **TCP Layer Connection to ECMG 1 Failed** minor alarm occurs when the Netcrypt has not established a TCP/IP link with the Primary ECMG. This alarm will only be sent again one time if the TCP/IP link is established with the Primary ECMG and then subsequently fails.

There is a potential for loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the Netcrypt that is sending this alarm. This alarm also indicates that the signal is being transmitted in the clear, when it should be encrypted.

Note: The Netcrypt will alternately seek to establish a TCP/IP link and a communication links with the Primary and Secondary ECMGs until one of the communication links succeeds. When a communication link is established, if any ECMG link/connection alarms are active, the Netcrypt clears those alarms.

Front Panel Message

None

Possible Cause(s)

- Cables are loose, disconnected, or defective.
- The ECMG is not operational.

Check and Correct

- 1 Check for loose connections or defective cables, tighten any loose cable connections, connect any disconnected cables, and replace any defective cables.
- 2 Check and verify that the ECMG is operating correctly.
- 3 If the alarm continues to occur, contact Cisco Services for further assistance.

Netcrypt Alarm ID 82 (52 Hex)

The Netcrypt **TCP Layer Connection to ECMG 2 Failed** minor alarm occurs when the Netcrypt has not established a TCP/IP link with the Primary ECMG. This alarm will only be sent again one time if the TCP/IP link is established with the Primary ECMG and then subsequently fails.

There is a potential for loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the Netcrypt that is sending this alarm. This alarm also indicates that the signal is being transmitted in the clear, when it should be encrypted.

Note: The Netcrypt will alternately seek to establish a TCP/IP link and a communication links with the Primary and Secondary ECMGs until one of the communication links succeeds. When a communication link is established, if any ECMG link/connection alarms are active, the Netcrypt clears those alarms.

Front Panel Message

None

Possible Cause(s)

- Cables are loose, disconnected, or defective.
- The ECMG is not operational.

Check and Correct

- 1 Check for loose connections or defective cables, tighten any loose cable connections, connect any disconnected cables, and replace any defective cables.
- 2 Check and verify that the ECMG is operating correctly.
- 3 If the alarm continues to occur, contact Cisco Services for further assistance.

Netcrypt Alarm ID 83 (53 Hex)

The Netcrypt **TCP Layer Connection to ECMG 3 Failed** minor alarm occurs when the Netcrypt has not established a TCP/IP link with the Primary ECMG. This alarm will only be sent again one time if the TCP/IP link is established with the Primary ECMG and then subsequently fails.

There is a potential for loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the Netcrypt that is sending this alarm. This alarm also indicates that the signal is being transmitted in the clear, when it should be encrypted.

Note: The Netcrypt will alternately seek to establish a TCP/IP link and a communication links with the Primary and Secondary ECMGs until one of the communication links succeeds. When a communication link is established, if any ECMG link/connection alarms are active, the Netcrypt clears those alarms.

Front Panel Message

None

Possible Cause(s)

- Cables are loose, disconnected, or defective.
- The ECMG is not operational.

Check and Correct

- 1 Check for loose connections or defective cables, tighten any loose cable connections, connect any disconnected cables, and replace any defective cables.
- 2 Check and verify that the ECMG is operating correctly.
- 3 If the alarm continues to occur, contact Cisco Services for further assistance.

Netcrypt Alarm ID 84 (54 Hex)

The Netcrypt **TCP Layer Connection to ECMG 4 Failed** minor alarm occurs when the Netcrypt has not established a TCP/IP link with the Primary ECMG. This alarm will only be sent again one time if the TCP/IP link is established with the Primary ECMG and then subsequently fails.

There is a potential for loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the Netcrypt that is sending this alarm. This alarm also indicates that the signal is being transmitted in the clear, when it should be encrypted.

Note: The Netcrypt will alternately seek to establish a TCP/IP link and a communication links with the Primary and Secondary ECMGs until one of the communication links succeeds. When a communication link is established, if any ECMG link/connection alarms are active, the Netcrypt clears those alarms.

Front Panel Message

None

Possible Cause(s)

- Cables are loose, disconnected, or defective.
- The ECMG is not operational.

Check and Correct

- 1 Check for loose connections or defective cables, tighten any loose cable connections, connect any disconnected cables, and replace any defective cables.
- 2 Check and verify that the ECMG is operating correctly.
- 3 If the alarm continues to occur, contact Cisco Services for further assistance.

Netcrypt Alarm ID 85 (55 Hex)

The Netcrypt **Application Layer Connection to ECMG 1 Failed** minor alarm occurs when the TCP/IP link is established, but the Netcrypt is unable to communicate with the Primary ECMG. This alarm remains active until the Primary ECMG establishes communication at which time it is deactivated. This alarm will only be sent again one time if the Primary ECMG establishes communication and subsequently fails. Connection to the Secondary ECMG is an available option.

There is a potential for loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the Netcrypt that is sending this alarm. This alarm also indicates that the signal is being transmitted in the clear, when it should be encrypted.

Note: The Netcrypt alternately seek to establish a TCP/IP link and a communication links with the Primary and Secondary ECMGs until one of the communication links succeeds. When a communication link is established, if any ECMG link/connection alarms are active, the Netcrypt clears those alarms.

Front Panel Message

None

Possible Cause(s)

- Cables are loose, disconnected, or defective.
- The primary ECMG connection parameters are incorrect.

Check and Correct

- 1 Check for loose connections or defective cables, tighten any loose cable connections, connect any disconnected cables, and replace any defective cables.
- 2 Check and verify the CAS ID parameters in the EC.
- 3 If the alarm continues to occur, contact Cisco Services for further assistance.

Netcrypt Alarm ID 86 (56 Hex)

The Netcrypt **Application Layer Connection to ECMG 2 Failed** minor alarm occurs when the TCP/IP link is established, but the Netcrypt is unable to communicate with the Primary ECMG. This alarm remains active until the Primary ECMG establishes communication at which time it is deactivated. This alarm will only be sent again one time if the Primary ECMG establishes communication and subsequently fails. Connection to the Secondary ECMG is an available option.

There is a potential for loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the Netcrypt that is sending this alarm. This alarm also indicates that the signal is being transmitted in the clear, when it should be encrypted.

Note: The Netcrypt alternately seek to establish a TCP/IP link and a communication links with the Primary and Secondary ECMGs until one of the communication links succeeds. When a communication link is established, if any ECMG link/connection alarms are active, the Netcrypt clears those alarms.

Front Panel Message

None

Possible Cause(s)

- Cables are loose, disconnected, or defective.
- The primary ECMG connection parameters are incorrect.

Check and Correct

- 1 Check for loose connections or defective cables, tighten any loose cable connections, connect any disconnected cables, and replace any defective cables.
- 2 Check and verify the CAS ID parameters in the EC.
- 3 If the alarm continues to occur, contact Cisco Services for further assistance.

Netcrypt Alarm ID 87 (57 Hex)

The Netcrypt **Application Layer Connection to ECMG 3 Failed** minor alarm occurs when the TCP/IP link is established, but the Netcrypt is unable to communicate with the Primary ECMG. This alarm remains active until the Primary ECMG establishes communication at which time it is deactivated. This alarm will only be sent again one time if the Primary ECMG establishes communication and subsequently fails. Connection to the Secondary ECMG is an available option.

There is a potential for loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the Netcrypt that is sending this alarm. This alarm also indicates that the signal is being transmitted in the clear, when it should be encrypted.

Note: The Netcrypt alternately seek to establish a TCP/IP link and a communication links with the Primary and Secondary ECMGs until one of the communication links succeeds. When a communication link is established, if any ECMG link/connection alarms are active, the Netcrypt clears those alarms.

Front Panel Message

None

Possible Cause(s)

- Cables are loose, disconnected, or defective.
- The primary ECMG connection parameters are incorrect.

Check and Correct

- 1 Check for loose connections or defective cables, tighten any loose cable connections, connect any disconnected cables, and replace any defective cables.
- 2 Check and verify the CAS ID parameters in the EC.
- 3 If the alarm continues to occur, contact Cisco Services for further assistance.

Netcrypt Alarm ID 88 (58 Hex)

The Netcrypt **Application Layer Connection to ECMG 4 Failed** minor alarm occurs when the TCP/IP link is established, but the Netcrypt is unable to communicate with the Primary ECMG. This alarm remains active until the Primary ECMG establishes communication at which time it is deactivated. This alarm will only be sent again one time if the Primary ECMG establishes communication and subsequently fails. Connection to the Secondary ECMG is an available option.

There is a potential for loss of programming content, macroblocking, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the Netcrypt that is sending this alarm. This alarm also indicates that the signal is being transmitted in the clear, when it should be encrypted.

Note: The Netcrypt alternately seek to establish a TCP/IP link and a communication links with the Primary and Secondary ECMGs until one of the communication links succeeds. When a communication link is established, if any ECMG link/connection alarms are active, the Netcrypt clears those alarms.

Front Panel Message

None

Possible Cause(s)

- Cables are loose, disconnected, or defective.
- The primary ECMG connection parameters are incorrect.

Check and Correct

- 1 Check for loose connections or defective cables, tighten any loose cable connections, connect any disconnected cables, and replace any defective cables.
- 2 Check and verify the CAS ID parameters in the EC.
- 3 If the alarm continues to occur, contact Cisco Services for further assistance.

Netcrypt Alarm ID 89 (59 Hex)

The Netcrypt **Received ECM for Non-Existent Session** minor alarm occurs when the Netcrypt receives SCG information for a session that does not exist on the Netcrypt. The Netcrypt clears this alarm immediately.

Front Panel Message

None

Possible Cause(s)

The parameters in the SCG message do not match any existing sessions provisioned on the Netcrypt.

Check and Correct

- 1 Check the SCS scheduler.
- 2 If the alarm continues to occur, contact Cisco Services for further assistance.

Netcrypt Alarm ID 99 (63 Hex)

The Netcrypt **Input 1 Gigabit Ethernet Autonegotiate Failure** minor alarm occurs when the Netcrypt fails to negotiate the specific link characteristics required to properly configure the link at initialization. Autonegotiation is a physical layer link configuration protocol that is used on the Netcrypt to select between duplex mode and the use of link level flow control.

Note: Autonegotiation protocol starts after the GigE cables are connected and the Netcrypt is powered up.

Front Panel Message

None

Possible Cause(s)

- A cable is loose, disconnected, or defective.
- The SFP may be defective
- The AutoNeg parameter on the chip may be set incorrectly

Check and Correct

A cable is loose, disconnected, or defective

Check for loose cable connections or defective cables at the inputs on the back panel of the Netcrypt, connect any disconnected cables, then tighten any loose cable connections, and replace any defective cables.

SFP may be defective

Replace the SFP with a replacement unit.

AutoNeg parameter incorrect

Verify the AutoNeg parameter by reading this value from the Netcrypt host application using the following Netcrypt Host Boot craft port commands:

- gmacr 0x18 for Port 0
- gmacr 0x98 for Port 1
- gmacr 0x118 for Port 2
- gmacr 0x198 for Port 3
- gmacr 0x218 for Port 4
- gmacr 0x298 for Port 5

Chapter 4 Netcrypt Alarms

- gmacr 0x318 for Port 6
- gmacr 0x398 for Port 7

Important! Verify that check Bit 5 of the return value = 1 for autonegotiation on.

Note: You can only use the preceding 'gmacr' commands at the **NC_HOST_BOOT>** prompt.



You can read the same values at the Netcrypt Host App prompt (**NC_HOST>**) using the following commands:

- peek 1 0x28C00060 // port 0
- peek 1 0x28C00260 // port 1
- peek 1 0x28C00460 // port 2
- peek 1 0x28C00660 // port 3
- peek 1 0x28C00860 // port 4
- peek 1 0x28C00A60 // port 5
- peek 1 0x28C00C60 // port 6
- peek 1 0x28C00E60 // port 7

Netcrypt Alarm ID 100 (64 Hex)

The Netcrypt **Input 2 Gigabit Ethernet Autonegotiate Failure** minor alarm occurs when the Netcrypt fails to negotiate the specific link characteristics required to properly configure the link at initialization. Autonegotiation is a physical layer link configuration protocol that is used on the Netcrypt to select between duplex mode and the use of link level flow control.

Note: Autonegotiation protocol starts after the GigE cables are connected and the Netcrypt is powered up.

Front Panel Message

None

Possible Cause(s)

- A cable is loose, disconnected, or defective.
- The SFP may be defective
- The AutoNeg parameter on the chip may be set incorrectly

Check and Correct

A cable is loose, disconnected, or defective

Check for loose cable connections or defective cables at the inputs on the back panel of the Netcrypt, connect any disconnected cables, then tighten any loose cable connections, and replace any defective cables.

SFP may be defective

Replace the SFP with a replacement unit.

AutoNeg parameter incorrect

Verify the AutoNeg parameter by reading this value from the Netcrypt host application using the following craft port commands:

- `gmacr 0x18` for Port 0
- `gmacr 0x98` for Port 1
- `gmacr 0x118` for Port 2
- `gmacr 0x198` for Port 3
- `gmacr 0x218` for Port 4
- `gmacr 0x298` for Port 5

Chapter 4 Netcrypt Alarms

- gmacr 0x318 for Port 6
- gmacr 0x398 for Port 7

Important! Verify that check Bit 5 of the return value = 1 for autonegotiation on.

Note: You can only use the preceding 'gmacr' commands at the **NC_HOST_BOOT>** prompt.



You can read the same values at the Netcrypt Host App prompt (**NC_HOST>**) using the following commands:

- peek 1 0x28C00060 // port 0
- peek 1 0x28C00260 // port 1
- peek 1 0x28C00460 // port 2
- peek 1 0x28C00660 // port 3
- peek 1 0x28C00860 // port 4
- peek 1 0x28C00A60 // port 5
- peek 1 0x28C00C60 // port 6
- peek 1 0x28C00E60 // port 7

Netcrypt Alarm ID 101 (65 Hex)

The Netcrypt **Input 3 Gigabit Ethernet Autonegotiate Failure** minor alarm occurs when the Netcrypt fails to negotiate the specific link characteristics required to properly configure the link at initialization. Autonegotiation is a physical layer link configuration protocol that is used on the Netcrypt to select between duplex mode and the use of link level flow control.

Note: Autonegotiation protocol starts after the GigE cables are connected and the Netcrypt is powered up.

Front Panel Message

None

Possible Cause(s)

- A cable is loose, disconnected, or defective.
- The SFP may be defective
- The AutoNeg parameter on the chip may be set incorrectly

Check and Correct

A cable is loose, disconnected, or defective

Check for loose cable connections or defective cables at the inputs on the back panel of the Netcrypt, connect any disconnected cables, then tighten any loose cable connections, and replace any defective cables.

SFP may be defective

Replace the SFP with a replacement unit.

AutoNeg parameter incorrect

Verify the AutoNeg parameter by reading this value from the Netcrypt host application using the following craft port commands:

- `gmacr 0x18` for Port 0
- `gmacr 0x98` for Port 1
- `gmacr 0x118` for Port 2
- `gmacr 0x198` for Port 3
- `gmacr 0x218` for Port 4
- `gmacr 0x298` for Port 5

Chapter 4 Netcrypt Alarms

- gmacr 0x318 for Port 6
- gmacr 0x398 for Port 7

Important! Verify that check Bit 5 of the return value = 1 for autonegotiation on.

Note: You can only use the preceding 'gmacr' commands at the **NC_HOST_BOOT>** prompt.



You can read the same values at the Netcrypt Host App prompt (**NC_HOST>**) using the following commands:

- peek 1 0x28C00060 // port 0
- peek 1 0x28C00260 // port 1
- peek 1 0x28C00460 // port 2
- peek 1 0x28C00660 // port 3
- peek 1 0x28C00860 // port 4
- peek 1 0x28C00A60 // port 5
- peek 1 0x28C00C60 // port 6
- peek 1 0x28C00E60 // port 7

Netcrypt Alarm ID 102 (66 Hex)

The Netcrypt **Input 4 Gigabit Ethernet Autonegotiate Failure** minor alarm occurs when the Netcrypt fails to negotiate the specific link characteristics required to properly configure the link at initialization. Autonegotiation is a physical layer link configuration protocol that is used on the Netcrypt to select between duplex mode and the use of link level flow control.

Note: Autonegotiation protocol starts after the GigE cables are connected and the Netcrypt is powered up.

Front Panel Message

None

Possible Cause(s)

- A cable is loose, disconnected, or defective.
- The SFP may be defective
- The AutoNeg parameter on the chip may be set incorrectly

Check and Correct

A cable is loose, disconnected, or defective

Check for loose cable connections or defective cables at the inputs on the back panel of the Netcrypt, connect any disconnected cables, then tighten any loose cable connections, and replace any defective cables.

SFP may be defective

Replace the SFP with a replacement unit.

AutoNeg parameter incorrect

Verify the AutoNeg parameter by reading this value from the Netcrypt host application using the following craft port commands:

- `gmacr 0x18` for Port 0
- `gmacr 0x98` for Port 1
- `gmacr 0x118` for Port 2
- `gmacr 0x198` for Port 3
- `gmacr 0x218` for Port 4
- `gmacr 0x298` for Port 5

Chapter 4 Netcrypt Alarms

- gmacr 0x318 for Port 6
- gmacr 0x398 for Port 7

Important! Verify that check Bit 5 of the return value = 1 for autonegotiation on.

Note: You can only use the preceding 'gmacr' commands at the NC_HOST_BOOT> prompt.



You can read the same values at the Netcrypt Host App prompt (NC_HOST>) using the following commands:

- peek 1 0x28C00060 // port 0
- peek 1 0x28C00260 // port 1
- peek 1 0x28C00460 // port 2
- peek 1 0x28C00660 // port 3
- peek 1 0x28C00860 // port 4
- peek 1 0x28C00A60 // port 5
- peek 1 0x28C00C60 // port 6
- peek 1 0x28C00E60 // port 7

Netcrypt Alarm ID 108 (6C Hex)

The Netcrypt **Input 1 PAT Update** minor alarm occurs when the PAT seen at port 1 yields a version number change indicating that the input stream has changed.

Front Panel Message

None

Possible Cause(s)

The input stream changed.

Check and Correct

There are two possible scenarios:

- If the Netcrypt handles the PAT update, the alarm is for information only. Nevertheless, you must manually acknowledge and clear the alarm to remove it from the alarm list. .
- If the Netcrypt does not handle the PAT update, the alarm is sent as a minor alarm, and does not clear. You may need to reboot the Netcrypt to re-acquire the input stream.

Netcrypt Alarm ID 109 (6D Hex)

The Netcrypt **Input 2 PAT Update** minor alarm occurs when the PAT seen at port 2 yields a version number change indicating that the input stream has changed.

Front Panel Message

None

Possible Cause(s)

The input stream changed.

Check and Correct

There are two possible scenarios:

- If the Netcrypt handles the PAT update, the alarm is for information only. Nevertheless, you must manually acknowledge and clear the alarm to remove it from the alarm list. .
- If the Netcrypt does not handle the PAT update, the alarm is sent as a minor alarm, and does not clear. You may need to reboot the Netcrypt to re-acquire the input stream.

Netcrypt Alarm ID 110 (6E Hex)

The Netcrypt **Input 3 PAT Update** minor alarm occurs when the PAT seen at port 3 yields a version number change indicating that the input stream has changed.

Front Panel Message

None

Possible Cause(s)

The input stream changed.

Check and Correct

There are two possible scenarios:

- If the Netcrypt handles the PAT update, the alarm is for information only. Nevertheless, you must manually acknowledge and clear the alarm to remove it from the alarm list. .
- If the Netcrypt does not handle the PAT update, the alarm is sent as a minor alarm, and does not clear. You may need to reboot the Netcrypt to re-acquire the input stream.

Netcrypt Alarm ID 111 (6F Hex)

The Netcrypt **Input 4 PAT Update** minor alarm occurs when the PAT seen at port 4 yields a version number change indicating that the input stream has changed.

Front Panel Message

None

Possible Cause(s)

The input stream changed.

Check and Correct

There are two possible scenarios:

- If the Netcrypt handles the PAT update, the alarm is for information only. Nevertheless, you must manually acknowledge and clear the alarm to remove it from the alarm list.
- If the Netcrypt does not handle the PAT update, the alarm is sent as a minor alarm, and does not clear. You may need to reboot the Netcrypt to re-acquire the input stream.

Netcrypt Alarm ID 116 (74 Hex)

The Netcrypt **Input 1 PMT Update** minor alarm occurs when the PMTs seen at port 1 yield a version number change indicating that the input stream has changed.

Front Panel Message

None

Possible Cause(s)

The input stream changed.

Check and Correct

If the Netcrypt handles the PMT update, the alarm is for information only. Nevertheless, you must manually acknowledge and clear the alarm to remove it from the alarm list.

If the Netcrypt does *not* handle the PMT update, the alarm is sent as a minor alarm, and does not clear. You may need to reboot the Netcrypt to re-acquire the input stream.

Netcrypt Alarm ID 117 (75 Hex)

The Netcrypt **Input 2 PMT Update** minor alarm occurs when the PMTs seen at port 2 yield a version number change indicating that the input stream has changed.

Front Panel Message

None

Possible Cause(s)

The input stream changed.

Check and Correct

- If the Netcrypt handles the PMT update, the alarm is for information only. Nevertheless, you must manually acknowledge and clear the alarm to remove it from the alarm list.
- If the Netcrypt does *not* handle the PMT update, the alarm is sent as a minor alarm, and does not clear. You may need to reboot the Netcrypt to re-acquire the input stream.

Netcrypt Alarm ID 118 (76 Hex)

The Netcrypt **Input 3 PMT Update** minor alarm occurs when the PMTs seen at port 3 yield a version number change indicating that the input stream has changed.

Front Panel Message

None

Possible Cause(s)

The input stream changed.

Check and Correct

- If the Netcrypt handles the PMT update, the alarm is for information only. Nevertheless, you must manually acknowledge and clear the alarm to remove it from the alarm list.
- If the Netcrypt does *not* handle the PMT update, the alarm is sent as a minor alarm, and does not clear. You may need to reboot the Netcrypt to re-acquire the input stream.

Netcrypt Alarm ID 119 (77 Hex)

The **Netcrypt Input 4 PMT Update** minor alarm occurs when the PMTs seen at port 4 yield a version number change indicating that the input stream has changed.

Front Panel Message

None

Possible Cause(s)

The input stream changed.

Check and Correct

- If the Netcrypt handles the PMT update, the alarm is for information only. Nevertheless, you must manually acknowledge and clear the alarm to remove it from the alarm list.
- If the Netcrypt does *not* handle the PMT update, the alarm is sent as a minor alarm, and does not clear. You may need to reboot the Netcrypt to re-acquire the input stream.

Netcrypt Alarm ID 120 (78 Hex)

The Netcrypt **Input 5 PMT Update** minor alarm occurs when the PMTs seen at port 5 yield a version number change indicating that the input stream has changed.

Front Panel Message

None

Possible Cause(s)

The input stream changed.

Check and Correct

- If the Netcrypt handles the PMT update, the alarm is for information only. Nevertheless, you must manually acknowledge and clear the alarm to remove it from the alarm list.
- If the Netcrypt does *not* handle the PMT update, the alarm is sent as a minor alarm, and does not clear. You may need to reboot the Netcrypt to re-acquire the input stream.

Netcrypt Alarm ID 121 (79 Hex)

The Netcrypt **Input 6 PMT Update** alarm occurs when the PMTs seen at port 6 yield a version number change indicating that the input stream has changed.

Front Panel Message

None

Possible Cause(s)

The input stream changed.

Check and Correct

- If the Netcrypt handles the PMT update, the alarm is for information only. Nevertheless, you must manually acknowledge and clear the alarm to remove it from the alarm list.
- If the Netcrypt does *not* handle the PMT update, the alarm is sent as a minor alarm, and does not clear. You may need to reboot the Netcrypt to re-acquire the input stream.

Netcrypt Alarm ID 122 (7A Hex)

The Netcrypt **Input 7 PMT Update** alarm occurs when the PMTs seen at port 7 yield a version number change indicating that the input stream has changed.

Front Panel Message

None

Possible Cause(s)

The input stream changed.

Check and Correct

- If the Netcrypt handles the PMT update, the alarm is for information only. Nevertheless, you must manually acknowledge and clear the alarm to remove it from the alarm list.
- If the Netcrypt does *not* handle the PMT update, the alarm is sent as a minor alarm, and does not clear. You may need to reboot the Netcrypt to re-acquire the input stream.

Netcrypt Alarm ID 123 (7B Hex)

The Netcrypt **Input 8 PMT Update** alarm occurs when the PMTs seen at port 8 yield a version number change indicating that the input stream has changed.

Front Panel Message

None

Possible Cause(s)

The input stream changed.

Check and Correct

- If the Netcrypt handles the PMT update, the alarm is for information only. Nevertheless, you must manually acknowledge and clear the alarm to remove it from the alarm list.
- If the Netcrypt does *not* handle the PMT update, the alarm is sent as a minor alarm, and does not clear. You may need to reboot the Netcrypt to re-acquire the input stream.

Netcrypt Alarm ID 124 (7C Hex)

The Netcrypt **Fan 1 Failure** minor alarm occurs when ventilation fan #1 on the side panel of the Netcrypt fails. You must replace the fan unit immediately to prevent the Netcrypt from overheating.

Note: There are five fan units on the side panel of the Netcrypt.

Front Panel Message

None

Possible Cause(s)

One of the fan units failed.

Check and Correct

Replace the fan unit that has failed. Contact your Cisco North American Marketing Manager to arrange for a genuine replacement fan unit. To properly install the fan unit, follow the installation instructions that ship with the replacement fan unit.

Netcrypt Alarm ID 125 (7D Hex)

The Netcrypt **Fan 2 Failure** minor alarm occurs when ventilation fan #2 on the side panel of the Netcrypt fails. You must replace the fan unit immediately to prevent the Netcrypt from overheating.

Note: There are five fan units on the side panel of the Netcrypt.

Front Panel Message

None

Possible Cause(s)

One of the fan units failed.

Check and Correct

Replace the fan unit that has failed. Contact your Cisco North American Marketing Manager to arrange for a genuine replacement fan unit. To properly install the fan unit, follow the installation instructions that ship with the replacement fan unit.

Netcrypt Alarm ID 126 (7E Hex)

The Netcrypt **Fan 3 Failure** alarm occurs when ventilation fan #3 on the side panel of the Netcrypt fails. You must replace the fan unit immediately to prevent the Netcrypt from overheating.

Note: There are five fan units on the side panel of the Netcrypt.

Front Panel Message

None

Possible Cause(s)

One of the fan units failed.

Check and Correct

Replace the fan unit that has failed. Contact your Cisco North American Marketing Manager to arrange for a genuine replacement fan unit. To properly install the fan unit, follow the installation instructions that ship with the replacement fan unit.

Netcrypt Alarm ID 127 (7F Hex)

The Netcrypt **Fan 4 Failure** minor alarm occurs when ventilation fan #4 on the side panel of the Netcrypt fails. You must replace the fan unit immediately to prevent the Netcrypt from overheating.

Note: There are five fan units on the side panel of the Netcrypt.

Front Panel Message

None

Possible Cause(s)

One of the fan units failed.

Check and Correct

Replace the fan unit that has failed. Contact your Cisco North American Marketing Manager to arrange for a genuine replacement fan unit. To properly install the fan unit, follow the installation instructions that ship with the replacement fan unit.

Netcrypt Alarm ID 128 (80 Hex)

The Netcrypt **Fan 5 Failure** minor alarm occurs when ventilation fan #5 on the side panel of the Netcrypt fails. You must replace the fan unit immediately to prevent the Netcrypt from overheating.

Note: There are five fan units on the side panel of the Netcrypt.

Front Panel Message

None

Possible Cause(s)

One of the fan units failed.

Check and Correct

Replace the fan unit that has failed. Contact your Cisco North American Marketing Manager to arrange for a genuine replacement fan unit. To properly install the fan unit, follow the installation instructions that ship with the replacement fan unit.

Netcrypt Alarm ID 129 (81 Hex)

The Netcrypt **Power Supply Failure** minor alarm occurs when the internal power supply on the Netcrypt fails or is failing.

Front Panel Message

None

Possible Cause(s)

The internal power supply on the Netcrypt has failed or is failing.

Check and Correct

- 1 Check power source, power wires, and the on/off rocker-type switch on the back panel of the Netcrypt.
- 2 Replace the Netcrypt if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the Netcrypt.
- 3 Contact Cisco Services for further assistance.

Netcrypt Alarm ID 256 (100 Hex) through Alarm ID 4255 (109F Hex)

The Netcrypt **Session Data Error** minor alarm occurs when the Netcrypt detects a session data error and indicates one of the following conditions:

- Underflow and overflow errors indicate that the data flow for the session is more or less than what has been defined by the EC for the session.
Important! The default threshold for the underflow and overflow alarms is zero. Note that the same threshold parameter is utilized for determining both underflow and overflow. The algorithm for determining underflow/overflow is as follows:
- When the threshold value is not provisioned by a management entity, the threshold value is 0 and the UNDERFLOW alarm will occur if the session's data rate falls below 1 bit per second (bps) (i.e., either equal to 0 bps or a fractional value that is less than 1 bps). In other words, the Overflow alarm is essentially disabled.
- When a management entity provisions the alarm with a non-zero threshold value, the UNDERFLOW alarm occurs when the measured session data rate falls below (sessionRate - threshold) and the OVERFLOW alarm occurs when the measured session data rate exceeds (sessionRate + threshold).
Note: sessionRate is the rate that was specified createSession request.
- PID enable errors indicate that a PID for this session is not enabled in the Netcrypt.
Note: A PID is contained in the MPEG header to link MPEG packets together.
- Continuity error.
- PLL unlocked
- Excess glue frame events

Alarm IDs 256 (decimal) through 4255 (decimal) represent Session Data alarms. Sessions correspond to MPEG programs. Each of these sessions will generate a unique Alarm ID when a Session Data Error occurs for that session.

Session data alarms for internal session indices 0 through 3999 on the Netcrypt are mapped to session data error Alarm IDs 256 (decimal) through 4255 (decimal).

Important! The **Additional Information** field in the Alarm Manager window displays the Session ID number, the port number, and the following Cause Codes for the Netcrypt Session Data Error:

- Cause Code 1=Underflow
- Cause Code 2=Overflow
- Cause Code 3=PID enable error

Chapter 4 Netcrypt Alarms

- Cause Code 6=Continuity error
- Cause Code 7=PLL unlocked
- Cause Code 8=Excess glue frame events

There is potential loss of programming content, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the Netcrypt that is sending this alarm.

Front Panel Message

None

Possible Cause(s)

The data flow for the session is lesser than or greater than what is defined by the EC for the session. This indicates one or more of the following underflow and overflow conditions:

- Cause Code 1 - Underflow conditions - The session data rate for this session drops to 0 (zero) or is less than expected.
Important! The session rate dropping to 0 (zero) triggers an underflow alarm, but is not the result of a loss of signal condition. When a loss of signal occurs, the underflow alarm is not reported. This prevents the system from being overwhelmed with a large number of session data alarms. Alarms that occur as a result of higher level alarms are not reported.
- Cause Code 2 - Overflow conditions - The data rate for this session exceeds the provisioned data rate.
- Cause Code 3 - PID enable error - A PID that should be enabled is not enabled in the Netcrypt.
- Cause Code 6 - Continuity error - This alarm identifies the specific session on which the Input Port (1-8) continuity error alarm occurred
- Cause Code 7 - PLL unlocked - The phase lock loop is unlocked for the given session.
- Cause Code 8 - Excess glue frame events - Glue frames prevent macroblocking. Excess glue frame events indicate that the associated output port is receiving too much data. When the MPEG engine in the Netcrypt nears full output capacity, it begins to selectively choose video PIDs on which it will issue a "freeze frame" code in the MPEG video stream for that program. Then the device drops the video packets for that session momentarily. This will happen only for sessions for which glue framing was enabled when the session was created. If this alarm occurs frequently, it is a signal that the output QAM carrying that session contains too much data.

Netcrypt Alarm ID 256 (100 Hex) through Alarm ID 4255 (109F Hex)

Check and Correct

Overflow and underflow conditions

- 1 Verify and correct any session setup problems, including the session rate target values.
Note: Select data rates that you believe the program should not exceed.
- 2 For the overflow condition, teardown, rebuild, and then restart the session using a higher bandwidth.
- 3 If the session setup data is correct, the data may be corrupt.
- 4 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 5 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report. If you cannot resolve these issues, contact Cisco Services.

PID enable issues

- If this alarm occurs with this Cause Code and then quickly clears, it is not a cause for concern.
- If the alarm does not quickly clear, verify and enable the PID in the Netcrypt.

Continuity error

Contact Cisco Services for further assistance.

PLL unlocked

Contact Cisco Services for further assistance.

Excess glue frame events

Reallocate the session from the modulator (QAM, MQAM, or GQAM) that appears to have too many sessions to another modulator on the same Netcrypt or to another Netcrypt.

Netcrypt Alarm ID 4256 (10A0) Hex) through Alarm ID 8255 (203F) Hex

The Netcrypt **Session Program Error** minor alarm occurs when there are errors or other problems in the input source for the session.

Alarm IDs 4256 (decimal) through 8255 (decimal) represent Session Program Error alarms. Sessions correspond to MPEG programs. Each of these sessions will generate a unique Alarm ID when a Session Program Error occurs for that session.

Session program alarms for internal session indices 0 through 3999 on the Netcrypt are mapped to session program Alarm IDs 4256 (decimal) through 8255 (decimal).

There is a potential for loss of programming content, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the Netcrypt that is sending this alarm.

Important! The **Additional Information** field in the Alarm Manager window displays the Session ID number, the port number, and the following Cause Codes for the Netcrypt Session Program Error:

- Cause Code 1=CRC error detected on a PMT
- Cause Code 2=New PMT detected
- Cause Code 3=Attempt to create a session failed

Front Panel Message

None

Possible Cause(s)

- Cause Code 1 - A CRC error was detected on a PMT.
- Cause Code 2 - A new PMT was detected.
- Cause Code 3 - An attempt to create a session failed.
- The PSI table data for the session contains errors.

Check and Correct

CRC error detected

Delete the session

Netcrypt Alarm ID 4256 (10A0) Hex) through Alarm ID 8255 (203F) Hex

New PMT detected

This is for information only. No action is required.

Create a session failed

Teardown and rebuild the session.

PSI table contains errors

Check the upstream MPEG input sources connected to the Netcrypt.

Netcrypt Alarm ID 8256 (2040 Hex) through Alarm ID 12255 (2FDF Hex)

The Netcrypt **Session Conditional Access Error** minor alarm occurs when the Netcrypt detects an error in the CA encryption for a session. This alarm indicates that the signal is being transmitted in the clear, when it should be encrypted.

Alarm IDs 8256 (decimal) through 12255 (decimal) represent Session Conditional Access alarms. Sessions correspond to MPEG programs. Each of these sessions will generate a unique Alarm ID when a Session Conditional Access Error occurs.

Session CA alarms for internal session indices 0 through 3999 on the Netcrypt are mapped to the session CA alarm IDs 8256 (decimal) through 12255 (decimal).

Important! When this condition exists, certain sessions may be broadcast without encryption, impacting potential pay-per-view and subscription revenues, and resulting in some subscribers receiving channels and services they do not want.

There is a potential for loss of programming content, black screens, tiling, freeze frames, poor video quality, and other degradations to service relative to the Netcrypt that is sending this alarm.

Important! The **Additional Information** field in the Alarm Manager window displays the Session ID number and the port number.

Front Panel Message

None

Possible Cause(s)

- CA failed.
- The CA settings are improper.
- A bad ISK VOD session.
- A hardware failure occurred.

Check and Correct

CA failed

Delete the failed session.

CA settings improper

Check and correct the CA settings on the EC.

Netcrypt Alarm ID 8256 (2040 Hex) through Alarm ID 12255 (2FDF Hex)

Bad ISK message

- 1 Troubleshoot CA on the EC.
- 2 Contact Cisco Services.

Hardware failure

- 1 Replace the Netcrypt if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the Netcrypt.
- 2 Contact Cisco Services for further assistance.

5

QPSK Modulator Alarms

Introduction

This chapter provides detailed information for troubleshooting the alarms that are generated by the QPSK modulator. The alarms are arranged in the ascending numeric order of the Alarm IDs. For your convenience, the Alarm IDs are listed in both decimal and hexadecimal format. You can look up the possible causes and then follow the check and correct procedures for each alarm to help you troubleshoot and clear each alarm.

Note: The actual alarm IDs sent by QPSK modulators are large hexadecimal numbers that start with "5001." For usability purposes, the QPSK modulator alarms presented to users were shortened by dropping the leading numeric string "5001." In order to derive the actual hexadecimal alarm ID that the QPSK modulator sends, add the hexadecimal alarm ID shown to the base hexadecimal value "50010000."

Example: For Alarm ID 256 (100 Hex), you would add the number 100 to the base hexadecimal value 50010000 to calculate the actual hexadecimal ID sent by the QPSK modulator, which is 50010100.

QPSK Modulator Alarm ID 0 (0 Hex)

The **QPSK Reboot** status event occurs during the boot-up process or when the QPSK modulator reboots because of a loss of electrical power or a manual reset. There is a temporary loss of services from the QPSK modulator that is sending this event until it returns to full service.

Note: This could be an intentional or an unintentional occurrence.

Front Panel Message

QPSK Reboot

Possible Cause(s)

- The QPSK modulator is rebooting.
- A user or system operator resets the QPSK modulator.
- A loss of power occurred.
- There is a problem in the DBDS

Check and Correct

Check the following items:

- 1 Verify that there are still broadcast services on this QPSK modulator.
- 2 Verify that the reset did not adversely affect broadcast services.
- 3 If the alarm continues to occur, contact Cisco Services for further assistance.

QPSK Modulator Alarm ID 1 (1 Hex)

The **Frequency Changed** status event occurs when a user or system operator changes a frequency setting on the QPSK modulator from the front panel or from the EC. There is a possible loss of services from the QPSK modulator that is sending this event.

Front Panel Message

Frequency changed

Possible Cause(s)

A user or a system operator changed the frequency setting on a QPSK modulator.

Check and Correct

- 1 Verify what settings were changed.
- 2 Are all services functioning correctly?
 - If **yes**, no further action is required.
 - If **no**, go to step 3.
- 3 Restore the settings to the previous configuration.
- 4 Manually power off and then power on the QPSK modulator, or reset the QPSK modulator to restore the previous configuration.
- 5 If resetting the QPSK modulator does not solve the problem, contact Cisco Services for further assistance.

QPSK Modulator Alarm ID 2 (2 Hex)

The **RF Level Changed** status event occurs when a user or a system operator changes the RF power level on the QPSK modulator. There is a possible loss of services from the QPSK modulator that is sending this event.

Front Panel Message

RF level changed

Possible Cause(s)

A user or a system operator changed the RF setting on a QPSK modulator.

Check and Correct

- 1 Verify what settings were changed.
- 2 Are all services functioning correctly?
 - If **yes**, no further action is required.
 - If **no**, go to step 3
- 3 Restore the settings to the previous configuration.
- 4 Manually power off and then power on the QPSK modulator, or reset the QPSK modulator to restore the previous configuration.
- 5 If resetting the QPSK modulator does not solve the problem, contact Cisco Services for further assistance.

QPSK Modulator Alarm ID 3 (3 Hex)

The **Front Panel Locked** alarm occurs when the front panel on the QPSK modulator is locked and someone presses a key on the front panel. When the front panel is locked, you cannot use the front panel keys to change settings.

Notes:

- Front Panel Lock may be set intentionally to prevent the settings being changed using the front panel keys.
- This alarm clears automatically when the front panel keys are not pressed.

Front Panel Message

Front Panel is locked

Possible Cause(s)

Front Panel Lock is selected in the EC Set Up QPSK Modulator window.

Check and Correct

Changing the Front Panel Lock Settings on the EC

Follow these steps to change the Front Panel Lock settings on the EC.

1. From the EC Administrative Console, select the **EC** tab.
2. Select the **Element Provisioning** tab.
3. Select **QPSK**. The QPSK List window appears.
4. From the QPSK List window, double-click the QPSK modulator you are modifying. The Set Up QPSK Modulator window appears.
5. Examine the box to the left of **Front Panel Lock** in the Options area of the window. If a check mark appears, click to deselect the check mark.
6. Click **Save**. The system saves the settings and the Set Up QPSK Modulator window closes.
7. Manually power off and then power on the QPSK modulator, or reset the QPSK modulator from the EC.
8. If resetting the QPSK modulator does not solve the problem, contact Cisco Services for further assistance.

QPSK Modulator Alarm ID 4 (4 Hex)

The **CW Mode On** alarm occurs when the QPSK modulator is in unmodulated CW carrier mode. Unmodulated CW carrier mode is used for configuration and testing. Modulated CW carrier mode is used for normal operation. When this condition exists, no services are available from this QPSK modulator.

Front Panel Message

CW mode changed from FP

Possible Cause(s)

- **Continuous Wave Mode** is selected in the EC Set Up QPSK Modulator window.
- **CW mode** was set to **Carrier Mode Unmodulated** using the front panel keys on the QPSK modulator.

Check and Correct

Change the Continuous Wave Mode settings on the EC

Follow these steps to change the CW mode on the EC.

1. From the EC Administrative Console, select the **EC** tab.
2. Select the **Element Provisioning** tab.
3. Select **QPSK**. The QPSK List window appears.
4. From the QPSK List window, double-click the QPSK modulator you are modifying. The Set Up QPSK Modulator window appears.
5. Examine the box to the left of **Continuous Wave Mode** in the Options area of the window. If it is checked, click it to remove the check.
6. Click **Save**. The system saves the settings and the Set Up QPSK Modulator window closes.
7. Manually power down, power up the QPSK modulator, or reset the QPSK modulator from the EC.
8. If resetting the QPSK modulator does not solve the problem, contact Cisco Services for further assistance.

Change the CW Mode Settings using the front panel keys

Follow these steps to change the CW mode to **Carrier Mode Modulated** using the front panel keys on the QPSK modulator.

1. Press the **CW** key one time to examine the CW setting on the front panel LCD screen.
2. Does the CW setting display as **Carrier Mode Unmodulated**?
 - If **no**, press the **Enter** key to exit and return to the default status screen.
 - If **yes**, use the up/down arrow keys located on the front panel of the QPSK modulator to set the Carrier mode to **Carrier Mode Modulated** on the LCD screen, and then press the **Enter** key to save the setting and return to the default status screen.

Result: The CW carrier mode is now set to modulated for normal operation.

Notes:

- Setting the Carrier Mode to **modulated** from the front panel when it was configured as **unmodulated** from the EC does not cause any alarms.
- If the Carrier mode is configured as **unmodulated** from the EC, subsequent reboots of the QPSK modulator will result in the Carrier Mode being configured as **unmodulated**.

QPSK Modulator Alarm ID 5 (5 Hex)

The **Front Panel Mute On** alarm occurs when the RF output on the back panel of the QPSK modulator is muted. When the RF output is muted, there is no RF output. This setting is used primarily to block output to the network during testing of the QPSK modulator. When this condition exists, no services are available from this QPSK modulator.

Front Panel Message

RF output is muted.

Possible Cause(s)

- **Mute RF Output** is selected in the EC Set Up QPSK Modulator window.
- **RF Output Mute** was set to **muted** using the front panel keys on the QPSK modulator.

Check and Correct

Change the Mute RF Output settings on the EC

1. From the EC Administrative Console, select the **EC** tab.
2. Select the **Element Provisioning** tab.
3. Select **QPSK**. The QPSK List window appears.
4. From the QPSK List window, double-click the QPSK modulator you are modifying. The Set Up QPSK Modulator window appears.
5. Examine the box to the left of **Mute RF Output** in the Options area of the window. If a check mark appears, click to deselect the check mark.
6. Click **Save**. The system saves the settings and the Set Up QPSK Modulator window closes.
7. Manually power off and then power on the QPSK modulator, or reset the QPSK modulator from the EC.
8. If resetting the QPSK modulator does not solve the problem, contact Cisco Services for further assistance.

Change the RF Output Mute settings using the front panel keys

Follow these steps to change the RF Output Mute settings using the front panel keys.

1. Press the Options key located on the QPSK modulator front panel four times to examine the RF Output Mute setting on the LCD screen.
2. Does the RF Output Mute display as muted?
 - If **no**, press the Enter key to exit and return to the default status screen.
 - If **yes**, use the up/down arrow keys to select unmuted and press the Enter key to save the setting and return to the default status screen.

Result: RF Output Mute is now set to unmuted for normal operation.

Notes:

- Setting the RF Output Mute to **unmuted** from the front panel when it was configured as muted from the EC does not cause any alarms.
- If the RF Output Mute is configured as **muted** from the EC, subsequent reboots of the QPSK modulator will result in the RF Output Mute being configured as **muted**.

QPSK Modulator Alarm ID 7 (7 Hex)

The **RF Not Locked** alarm occurs when the QPSK modulator detects that one of the two phase-locked loops is not locked on the output converter. This suppresses the RF output. When this condition exists, no services are available from this QPSK modulator.

Front Panel Message

RF is not locked

Possible Cause(s)

The QPSK modulator has failed or is failing.

Check and Correct

- 1 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 2 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 3 Replace the QPSK modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the QPSK modulator.
- 4 If you cannot resolve the issues that are identified in the Doctor Report, contact Cisco Services.

QPSK Modulator Alarm 256 (100 Hex)

The **Provisioning Data Not Received** alarm occurs when the QPSK modulator fails to receive provisioning data from the EC qpskManager process. When the QPSK modulator boots, it sends a request to the EC qpskManager process for provisioning data. If this data is not received within a certain amount of time, the QPSK modulator generates this alarm. When this condition exists, no services are available from this QPSK modulator.

Front Panel Message

QPSK provision failed

Possible Cause(s)

- The QPSK modulator failed to connect to the EC qpskManager process.
- This alarm also occurs and displays only on the front panel of the QPSK modulator, if the Ethernet cable is removed or disconnected after bootp processing completes. This alarm will clear automatically when the cable is re-connected.

Check and Correct

Verify the EC qpskManager process

Follow these steps to verify that the EC qpskManager process is running.

- 1 In the EC Administrative Console Status window, click **Monitor** in the EC area of the window. The EC Monitor screen appears on the right of the screen.
- 2 Is the indicator to the left of qpskManager illuminated green?
 - If **yes**, the qpskManager is running. You have completed this procedure.
 - If **no**, go to step 3.
- 3 From an xterm window on the EC, type **dncsControl** and press **Enter**. The Dncs Control window opens.
- 4 Type **2** (for Startup/Shutdown Single Element Group) and press **Enter**. The EC Startup/Shutdown Element Group selection list appears in the Dncs Control window.
- 5 Type **3** (for QPSK Managers) and press **Enter**. The target status for element group selection list appears in the Dncs Control window.
- 6 Type **e** (for Display Element Entries) and press **Enter**. The Startup/Shutdown Single Element Item selection list appears in the Dncs Control window.
- 7 Type **4** (for QPSK Managers) and press **Enter**. The target status for element selection list appears in the Dncs Control window.
- 8 Press **2** (for running) and press **Enter**. A confirmation message appears.

Chapter 5 QPSK Modulator Alarms

- 9 Type **y** (for yes) and then press **Enter**. The DnCS Control window refreshes.
Note: The DnCS Control window refreshes periodically, or you can press **Enter** to force a refresh.
- 10 Wait until **Curr Stt** (for current state) indicates running.
- 11 To exit, type **x** and press **Enter**.
- 12 Follow the on-screen instructions to close the DnCS Control window and to return to the xterm window.
- 13 Minimize the xterm window and look at the EC Monitor window to verify that the qpskManager process is now running.
- 14 Is the qpskManager process running?
 - If **yes**, you have completed this procedure.
 - If **no**, repeat this procedure from step 4, then go to step 15.
- 15 If the qpskManager process is still not running after repeating the procedure, run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 16 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 17 If you cannot resolve the issues that are identified in the Doctor Report, contact Cisco Services.

Check Ethernet cables

- 1 Check the QPSK modulator Ethernet connections to the EC and tighten any loose cables, connect any disconnected cables, then replace any defective cables.
- 2 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 3 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 4 Replace the QPSK modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the QPSK modulator.
- 5 If you cannot resolve the issues that are identified in the Doctor Report, contact Cisco Services.

QPSK Modulator Alarm ID 257 (101 Hex)

The **Not Connected to qpskManager** alarm occurs when the QPSK modulator does not have an RPC connection to the EC qpskManager process. When this condition exists, there is a potential for degradation to the services from this QPSK modulator.

Front Panel Message

No connect to QPSK Mgr.

Possible Cause(s)

- A cable is loose, disconnected, or defective.
- The RPC portmap request failed.
- The EC qpskManager process is not running.
- The QPSK modulator is failing.

Check and Correct

Check cable connections

Check for loose connections or defective cables, tighten any loose cable connections, connect any disconnected cables, and replace any defective cables.

Verify the Directory, Name, and Bootp Parameters for the Configuration File

Follow these steps to verify that the directory and name of the configuration file for the QPSK modulator, and to verify that the bootp parameters contained in the configuration file are correct.

Important! The default configuration file name is qpsk.config and the default location is the /tftpboot directory. Other locations and file names can be specified in the /etc/bootptab file.

- 1 Open an xterm window on the EC.
- 2 Type **cd /etc** and press **Enter**. The /etc directory becomes the working directory.
- 3 Type **more bootptab** and press **Enter**. The contents of the /etc/bootptab file appear.
- 4 Look for the “:td=” line and note the directory identified there. This line identifies the location of the configuration file.
- 5 Look for the “:bf=” line. This line identifies the configuration file name for the QPSK modulator.
- 6 Is there a line that contains an entry for “:bf=” in the /etc/bootptab file?
 - If **yes**, note the file name, and go to step 7.
 - If **no**, go to step 7.
- 7 Type **Ctrl C (^C)** and press **Enter** to exit the more utility.

Chapter 5 QPSK Modulator Alarms

- 8 Type **cd /<directory>** and press **Enter**. The /<directory> directory becomes the working directory.
Note: In this command, <directory> is the directory identified on the “:td=” line in the /etc/bootptab file.
- 9 Type **ls** and press **Enter**. A list of files in the /<directory> directory appears.
Note: The ‘l’ in “ls” is a lower case L.
- 10 Verify that either the qpsk.config file or the file identified on the “:bf=” line appears in the list of files.
- 11 Does the qpsk.config file appear in the list of files?
 - If **yes**, go to step 12.
 - If **no**, go to step 14.
- 12 Type **more qpsk.config** and press **Enter**. The Modulator/ Demodulator specific bootp parameters list appears.
- 13 Are the bootp parameters listed in the qpsk.config file correct?
 - If **yes**, you have completed this procedure.
 - If **no**, contact Cisco Services.
- 14 Does goqam appear in the list of files?
 - If **yes**, go to step 15
 - If **no**, contact Cisco Services.**Note:** In this command, goqam is the filename identified on the “:bf=” line in the /etc/bootptab file.
- 15 Type **more goqam** and press **Enter**. The Modulator/Demodulator specific bootp parameters list appears.
Note: In this command, goqam is the filename identified on the “:bf=” line in the /etc/bootptab file.
- 16 Are the bootp parameters listed in goqam correct?
 - If **yes**, you have completed this procedure.
 - If **no**, contact Cisco Services.

Verify that the EC qpskManager process is running

Check the QPSK modulator

- 1** If this alarm is reported by only one QPSK modulator, replace the QPSK modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the QPSK modulator.
- 2** If this alarm is reported by many QPSK modulators, follow these steps to troubleshoot the alarm.
 - a** Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
 - b** Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
 - c** Replace the QPSK modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the QPSK modulator.
 - d** If you cannot resolve the issues that are identified in the Doctor Report, contact Cisco Services.

QPSK Modulator Alarm ID 258 (102 Hex)

The **Not Connected to HCT Manager** alarm occurs when the QPSK modulator does not have an RPC connection to the EC HCT Manager processes. When this condition exists, some DHCTs will not reboot, and overall DHCT functionality is reduced.

Front Panel Message

No connect to Hct Mgr.

Possible Cause(s)

- A cable is loose, disconnected, or defective.
- The RPC portmap request failed.
- The EC HCT Manager processes are not running.
- The QPSK modulator is failing.

Check and Correct

Check for loose, disconnected, or defective cable connections

Check for loose connections or defective cables, tighten any loose cable connections, connect any disconnected cables, and replace any defective cables.

Verify the Directory, Name, and Bootp Parameters for the Configuration File

Verify the directory and name of the configuration file for the QPSK modulator, and verify that the bootp parameters contained in the configuration file are correct.

Important! The default configuration file name is `qpsk.config` and the default location is the `/tftpboot` directory. Other locations and file names can be specified in the `/etc/bootptab` file.

Verify the EC HCT Manager Processes

Follow these steps to verify that the HCT Manager processes are running on the EC.

Note: The four EC HCT Manager processes are:

- `hctmCache`
- `hctmConfig`
- `hctmMac`
- `hctmProvision`

- 1 In the EC Administrative Console Status window, click Monitor in the EC area of the window. The EC Monitor screen appears on the right of the screen.

- 2 Is the indicator to the left of the dnscsSnmpAgent process illuminated green?
 - If **yes**, the dnscsSnmpAgent process is running. You have completed this procedure.
 - If **no**, go to step 3.
- 3 From an xterm window on the EC, type **dnscsControl** and press **Enter**. The Dnscs Control window opens.
- 4 Type **2** (for Startup/Shutdown Single Element Group) and press **Enter**. The EC Startup/Shutdown Element Group selection list appears in the Dnscs Control window.
- 5 Type **4** (for HCT Manager) and press **Enter**. The target status for element group selection list appears in the Dnscs Control window.
- 6 Type **2** (for running) and press **Enter**. A confirmation message appears.
- 7 Type **y** (for yes) and press **Enter**. The Dnscs Control window refreshes.
- 8 Wait until **Curr Stt** (for current state) indicates running.
- 9 To exit, type **x** and press **Enter**.
- 10 Follow the on-screen instructions to close the Dnscs Control window and to return to the xterm window.
- 11 Minimize the xterm window and look at the EC Monitor window to verify that the indicator to the left of the dnscsSnmpAgent process is now illuminated green.
- 12 Is the indicator illuminated green?
 - If **yes**, you have completed this procedure.
 - If **no**, repeat this procedure from step 4, then go to step 13.
- 13 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services. Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 14 If you cannot resolve the issues that are identified in the Doctor Report, contact Cisco Services.

Chapter 5 QPSK Modulator Alarms

Check the QPSK modulator

- 1** If this alarm is reported by only one QPSK modulator, replace the QPSK modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the QPSK modulator.
- 2** If this alarm is reported by many QPSK modulators, follow these steps to troubleshoot the alarm.
 - a** Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
 - b** Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
 - c** Replace the QPSK modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the QPSK modulator.
 - d** If you cannot resolve the issues that are identified in the Doctor Report, contact Cisco Services.

QPSK Modulator Alarm ID 259 (103 Hex)

The **Not Connected to dnscsSnmpAgent** alarm occurs when the QPSK modulator does not have an RPC connection to the EC dnscsSnmpAgent process. When this condition exists, no alarms are sent to the EC SNMP Agent.

Important! In QPSK modulator software release versions beginning with version A63, this alarm this alarm is not set and is not sent to the EC.

Front Panel Message

No connect to Alarm Mgr.

Possible Cause(s)

- A cable is loose, disconnected, or defective.
- The RPC portmap request failed.
- The EC dnscsSnmpAgent process is not running.
- The QPSK modulator is failing.

Check and Correct

Check for loose, disconnected, or defective cables

Check for loose connections or defective cables, tighten any loose cable connections, connect any disconnected cables, and replace any defective cables.

Verify the Directory, Name, and Bootp Parameters for the Configuration File

Verify the directory and name of the configuration file for the QPSK modulator, and verify that the bootp parameters contained in the configuration file are correct.

Important! The default configuration file name is qpsk.config and the default location is the /tftpboot directory. Other locations and file names can be specified in the /etc/bootptab file.

Verify the dnscsSnmpAgent process on the EC

Follow these steps to verify that the dnscsSnmpAgent process on the EC is running.

- 1 In the EC Administrative Console Status window, click **Monitor** in the EC area of the window. The EC Monitor screen appears on the right of the screen.
- 2 Is the indicator to the left of the dnscsSnmpAgent process illuminated green?
 - If **yes**, the dnscsSnmpAgent process is running. You have completed this procedure.
 - If **no**, go to step 3.
- 3 From an xterm window on the EC, type **dnscsControl** and press **Enter**. The Dnscs Control window opens.

Chapter 5 QPSK Modulator Alarms

- 4 Type **2** (for Startup/Shutdown Single Element Group) and press **Enter**. The EC Startup/Shutdown Element Group selection list appears in the DnCS Control window.
- 5 Type **2** (for EC SNMP Agent) and press **Enter**. The target status for element group selection list appears in the DnCS Control window.
- 6 Type **e** (for Display Element Entries) and press **Enter**. The Startup/Shutdown Single Element Item selection list appears in the DnCS Control window.
- 7 Type **2** (for dnCSsnmpAgent) and press **Enter**. The target status for element selection list appears in the DnCS Control window.
- 8 Type **2** (for running) and press **Enter**. A confirmation message appears.
- 9 Type **y** (for yes) and press **Enter**. The DnCS Control window refreshes.
Note: The DnCS Control window refreshes periodically, or you can press **Enter** to force a refresh.
- 10 Wait until **Curr Stt** (for current state) indicates running.
- 11 To exit, type **x** and press **Enter**.
- 12 Follow the on-screen instructions to close the DnCS Control window and to return to the xterm window.
- 13 Minimize the xterm window and look at the EC Monitor window to verify that the indicator to the left of the dnCSsnmpAgent process is now illuminated green.
- 14 Is the indicator illuminated green?
 - If **yes**, you have completed this procedure.
 - If **no**, repeat this procedure from step 4, then go to step 15.
- 15 If the dnCSsnmpAgent process is still not running after repeating the procedure, run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 16 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 17 If you cannot resolve the issues that are identified in the Doctor Report, contact Cisco Services.

Check the QPSK modulator

- 1** If this alarm is reported by only one QPSK modulator, replace the QPSK modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing and repairing the QPSK modulator.
- 2** If this alarm is reported by many QPSK modulators, follow these steps to troubleshoot the alarm.
 - a** Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
 - b** Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
 - c** Replace the QPSK modulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the QPSK modulator.
 - d** If you cannot resolve the issues that are identified in the Doctor Report, contact Cisco Services.

QPSK Modulator Alarm ID 260 (104 Hex)

The **TFTP File Open Failed** alarm occurs when the QPSK modulator is unable to open one or more of the files referenced by the configuration file received in the bootp reply message from the EC. When this condition exists, no services are available from this QPSK modulator.

When the QPSK modulator boots, it sends out a bootp request in order to obtain the IP address of its Ethernet interface, as well as other configuration parameters. The EC provides these parameters in a bootp reply message to the QPSK modulator. By default, the configuration file (usually named `qpsk.config`) resides in the `/tftpboot` directory. However, entries can be made in the `/etc/bootptab` file on the line beginning with `“:td=“` to specify a different directory in which to look for the configuration file, and on the line beginning with `“:bf=“` to specify a different file name for the configuration file.

Notes:

- The bootp parameter file(s) contained in the default configuration file (`qpsk.config`) or in the file identified on the `“:bf=“` line, must exist in the default directory (`/tftpboot`) or in the directory identified on the `“:td=“` line.
- The bootp parameter file(s) must be correct and must have proper access permissions for this operation to succeed.

Front Panel Message

TFTP File Open Failed

Possible Cause(s)

The bootp parameter files contained in either the default configuration file (`qpsk.config`) or in the configuration file that is identified on the `“:bf=“` line in the `/etc/bootptab` file, do not exist in the proper directory, are incorrect, or do not have proper access permissions.

Check and Correct

- 1 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 2 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 3 If you cannot resolve the issues that are identified in the Doctor Report, contact Cisco Services.

QPSK Modulator Alarm ID 261 (105 Hex)

The **TFTP File Read Failed** alarm occurs when the QPSK modulator is unable to read one or more of the files referenced by the configuration file received in the bootp reply message from the EC. When this condition exists, no services are available from this QPSK modulator.

When the QPSK modulator boots, it sends out a bootp request in order to obtain the IP address of its Ethernet interface, as well as other configuration parameters. The EC provides these parameters in a bootp reply message to the QPSK modulator. By default, the configuration file (usually named `qpsk.config`) resides in the `/tftpboot` directory. However, entries can be made in the `/etc/bootptab` file on the line beginning with `:td=` to specify a different directory in which to look for the configuration file, and on the line beginning with `:bf=` to specify a different file name for the configuration file.

Notes:

- The bootp parameter file(s) contained in the default configuration file (`qpsk.config`) or in the file identified on the `:bf=` line, must exist in the default directory (`/tftpboot`) or in the directory identified on the `:td=` line.
- The bootp parameter file(s) must be correct and must have proper access permissions for this operation to succeed.

Front Panel Message

TFTP File Read Failed

Possible Cause(s)

The bootp parameter files contained in either the default configuration file (`qpsk.config`) or in the configuration file that is identified on the `:bf=` line in the `/etc/bootptab` file, do not exist in the proper directory, are incorrect, or do not have proper access permissions.

Check and Correct

- 1 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 2 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 3 If you cannot resolve the issues that are identified in the Doctor Report, contact Cisco Services.

QPSK Modulator Alarm ID 263 (107 Hex)

The **Bootp Reply Failure** alarm occurs when the QPSK modulator does not receive a reply from the EC when executing a bootp procedure. Because broadcast bootp protocol is used, it is likely that a connection is not present to the EC.

Front Panel message

Bootp Reply Failed

Possible Cause(s)

- The QPSK modulator timed out while waiting for a bootp reply from the EC.
- Excessive traffic on the EC network.

Check and Correct

QPSK modulator timed out

Check the QPSK modulator Ethernet connection to the EC, tighten any loose cables, and replace any defective cables.

Excessive network traffic

- 1 Use a Sniffer Analyzer to check EC Ethernet traffic levels.
- 2 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 3 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 4 Replace the QPSK modulator if you have a spare, and contact your Cisco North American Marketing Manager to arrange for repairing or replacing the QPSK modulator.
- 5 If you cannot resolve the issues that are identified in the Doctor Report, contact Cisco Services.

QPSK Modulator Alarm ID 264 (108 Hex)

The **Bootp File Open Failure** alarm occurs when the QPSK modulator is unable to open the configuration file referenced in the bootp reply message from the EC. When this condition exists, no services are available from this QPSK modulator.

When a QPSK modulator boots, it sends out a bootp request in order to obtain the IP address of its Ethernet interface, as well as other configuration parameters. The EC supplies these parameters in a bootp reply message to the QPSK modulator. By default, the configuration file (usually named `qpsk.config`) resides in the `/tftpboot` directory. However, entries can be made in the `/etc/bootptab` file on the line beginning with `“:td=“` to specify a different directory in which to look for the configuration file, and on the line beginning with `“:bf=“` to specify a different file name for the configuration file. Both the directory and the files must have proper permissions for this operation to succeed.

Front Panel Message

Bootp File Open Fail

Possible Cause(s)

- The default configuration file (`qpsk.config`) does not exist in the default or specified location, or the configuration file has a different name.
Important! The default configuration file name is `qpsk.config` and the default location is the `/tftpboot` directory. Other locations and file names could be specified in the `/etc/bootptab` file.
- The default directory (`/tftpboot`), or the directory identified on the `“:td=“` line in the `/etc/bootptab` file for the QPSK modulator, does not have proper access permissions.
- The default configuration file (`qpsk.config`), or the file identified on the `“:bf=“` line in the `/etc/bootptab` file for the QPSK modulator, does not have proper access permissions.
- The QPSK modulator software failed to install properly on the EC.

Check and Correct

Verify the Location and Name of the Configuration File

Follow these steps to verify that the default configuration file (qpsk.config) exists in the default directory (/tftpboot) or to verify that another location or file name for the configuration file is specified in the /etc/bootptab file.

Important! The default configuration file name is qpsk.config and the default location is the /tftpboot directory. Other locations and file names could be specified in the /etc/bootptab file.

- 1 In an xterm window on the EC type **cd /etc** and press **Enter**. The /etc directory becomes the working directory.
- 2 Type **more bootptab** and press **Enter**. The contents of the bootptab file appear.
- 3 Look for the line beginning with “:td=” and note the directory identified there. This line identifies the location of the configuration file for the QPSK modulator.
- 4 Look for a line beginning with “:bf=.” This line identifies the configuration file name for the QPSK modulator.
- 5 Is there a line that contains an entry for “:bf=” in the /etc/bootptab file?
 - If **yes**, note the file name, and go to step 6.
 - If **no**, go to step 6.
- 6 Type **Ctrl C (^C)** and press **Enter** to exit the more utility.
- 7 Type **cd /<directory>** and press **Enter**. The /<directory> directory becomes the working directory.

Note: In this command, <directory> is the directory identified on the “:td=” line in the /etc/bootptab file.
- 8 Type **ls** and press **Enter**. A list of files in the /<directory> directory appears.

Note: The “l” in “ls” is a lowercase L.
- 9 Does the default configuration file (qpsk.config) or the file identified on the “:bf=” line appear in the list of files?
 - If **yes**, go to **Verify Boot Directory Access Permissions**.
 - If **no**, contact Cisco Services.

Verify Boot Directory Access Permissions

Follow these steps to verify that the default directory (/tftpboot), or the directory identified on the “:td=” line in the /etc/bootptab file for the QPSK modulator has proper access permissions.

- 1 In an xterm window on the EC, type **cd /<directory>** and press **Enter**. The /<directory> directory becomes the working directory.

Note: In this command, <directory> is the directory identified on the “:td=” line in the /etc/bootptab file.
- 2 Type **ls -ld** and press **Enter**. The access permissions for the /<directory> directory display.

Note: The “l” in ls -ld is a lowercase L.

- 3 Are the access permissions for the /<directory> directory listed as - **drwx - xr - x** ?
 - If **yes**, go to Verifying the Configuration File Access Permissions, next in this section.
 - If **no**, go to step 4.
- 4 Log on to the EC as a root user and change the access permissions.

Note: A password is required. See your network administrator if you need to obtain the root password.
- 5 Type **chmod 755 <directory>** and press **Enter**. The system changes the directory access permissions to - **drwx - xr - x**.

Note: In this command <directory> is the directory identified on the “:td=” line in the /etc/bootptab file.
- 6 Type **ls -ld <directory>** and press **Enter** to confirm the change. The access permissions for the /<directory> directory display.

Note: The “l” in ls -ld is a lowercase L.
- 7 Are the access permissions for the /<directory> directory now listed as - **drwx - xr - x** ?
 - If **yes**, go to **Verify the Configuration File Access Permissions**.
 - If **no**, repeat this procedure once from step 4; then, if the access permissions for the /<directory> directory are still incorrect, contact Cisco Services.

Verify the Configuration File Access Permissions

Follow these steps to verify that the default configuration file (qpsk.config), or the file identified on the “:bf=” line in the /etc/bootptab file for the QPSK modulator has proper access permissions.

- 1 In an xterm window on the EC, type **cd /<directory>** and press **Enter**. The /<directory> becomes the working directory.

Note: In this command, <directory> is the directory identified on the “:td=” line in the /etc/bootptab file.
- 2 Type **ls -l goqam** and press **Enter**. The access permissions for the goqam file display.

Important! In this command, goqam is the name of the file identified on the “:bf=” line in the /etc/bootptab file, or it is the default configuration file (qpsk.config).

Note: The “l” in ls -l is a lowercase L.
- 3 Are the access permissions for the goqam file listed as - **rw - r - - r - -** ?
 - If **yes**, you have completed this procedure.
 - If **no**, go to step 4.
- 4 Log on to the EC as a **root** user and change the access permissions.

Note: A password is required. See your network administrator if you need to obtain the root password.

Chapter 5 QPSK Modulator Alarms

- 5 Type **chmod 644 goqam** and press **Enter**. The system changes the file access permissions to **-rw -r - -r - -**.
Note: In this command, goqam is the filename identified on the “:bf=” line in the /etc/bootptab file, or it is the default configuration file (qpsk.config).
- 6 Type **ls -l goqam** and press **Enter** to confirm the change. The access permissions for the goqam file display.
Note: The “l” in ls -l is a lowercase L.
- 7 Are the access permissions for the goqam file now listed as **-rw -r - -r - -**?
 - If **yes**, you have completed this procedure.
 - If **no**, repeat this procedure once from step 4; then, if the access permissions are still incorrect, contact Cisco Services.

Check software installation

- 1 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 2 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 3 Replace the QPSK modulator if you have a spare, and contact your Cisco North American Marketing Manager to arrange for replacing or repairing the QPSK modulator.
- 4 If you cannot resolve the issues that are identified in the Doctor Report, contact Cisco Services.

QPSK Modulator Alarm ID 265 (109 Hex)

The **Bootp File Read Failure** alarm occurs when the QPSK modulator is unable to read the configuration file referenced in the bootp reply message from the EC. When this condition exists, no services are available from this QPSK modulator.

When a QPSK modulator boots, it sends out a bootp request in order to obtain the IP address of its Ethernet interface, as well as other configuration parameters. The EC supplies these parameters in a bootp reply message to the QPSK modulator. By default, the configuration file (usually named `qpsk.config`) resides in the `/tftpboot` directory. However, entries can be made in the `/etc/bootptab` file on the line beginning with `“:td=”` specifying a different directory in which to look for the configuration file, and on the line beginning with `“:bf=”` specifying a different file name for the configuration file. Both the directory and the file(s) must have proper permissions for this operation to succeed.

Front Panel Message

Bootp File Read Fail

Possible Cause(s)

- The default directory (`/tftpboot`), or the directory identified on the `“:td=”` line in the `/etc/bootptab` file for the QPSK modulator, does not have proper access permissions.
- The default configuration file (`qpsk.config`), or the file identified on the `“:bf=”` line in the `/etc/bootptab` file for the QPSK modulator, does not have proper access permissions.
- The default configuration file (`qpsk.config`), or the file identified on the `“:bf=”` line in the `/etc/bootptab` file for the QPSK modulator, on the EC is corrupt.

Check and Correct

Verify Boot Directory Access Permissions

Follow these steps to verify that the default directory (`/tftpboot`), or the directory identified on the `“:td=”` line in the `/etc/bootptab` file for the QPSK modulator has proper access permissions.

- 1 In an xterm window on the EC, type `cd /<directory>` and press **Enter**. The `/<directory>` directory becomes the working directory.
Note: In this command, `<directory>` is the directory identified on the `“:td=”` line in the `/etc/bootptab` file.
- 2 Type `ls -ld` and press **Enter**. The access permissions for the `/<directory>` directory display.
Note: The `“l”` in `ls -ld` is a lowercase L.

Chapter 5 QPSK Modulator Alarms

- 3 Are the access permissions for the /<directory> directory listed as **- drwx - xr - x** ?
 - If **yes**, go to Verify the Configuration File Access Permissions.
 - If **no**, go to step 4.
- 4 Log on to the EC as a **root** user and change the access permissions.
Note: A password is required. See your network administrator if you need to obtain the root password.
- 5 Type **chmod 755 <directory>** and press **Enter**. The system changes the directory access permissions to **- drwx - xr - x**.
Note: In this command <directory> is the directory identified on the “:td=” line in the /etc/bootptab file.
- 6 Type **ls -ld <directory>** and press **Enter** to confirm the change. The access permissions for the /<directory> directory display.
Note: The “l” in ls -ld is a lowercase L.
- 7 Are the access permissions for the /<directory> directory now listed as **- drwx - xr - x** ?
 - If **yes**, go to Verify the Configuration File Access Permissions.
 - If **no**, repeat this procedure once from step 4; then, if the access permissions for the /<directory> directory are still incorrect, contact Cisco Services.

Verify the Configuration File Access Permissions

Follow these steps to verify that the default configuration file (qpsk.config), or the file identified on the “:bf=” line in the /etc/bootptab file for the QPSK modulator has proper access permissions.

- 1 In an xterm window on the EC, type **cd /<directory>** and press **Enter**. The /<directory> becomes the working directory.
Note: In this command, <directory> is the directory identified on the “:td=” line in the /etc/bootptab file.
- 2 Type **ls -l goqam** and press **Enter**. The access permissions for the goqam file display.
Important! In this command, goqam is the name of the file identified on the “:bf=” line in the /etc/bootptab file, or it is the default configuration file (qpsk.config).
Note: The “l” in ls -l is a lowercase L.
- 3 Are the access permissions for the goqam file listed as **- rw - r - - r - - ?**
 - If **yes**, you have completed this procedure.
 - If **no**, go to step 4.
- 4 Log on to the EC as a **root** user and change the access permissions.
Note: A password is required. See your network administrator if you need to obtain the root password.

- 5 Type **chmod 644 goqam** and press **Enter**. The system changes the file access permissions to **-rw -r - -r - -**.
Note: In this command, goqam is the filename identified on the “:bf=” line in the /etc/bootptab file, or it is the default configuration file (qpsk.config).
- 6 Type **ls -l goqam** and press **Enter** to confirm the change. The access permissions for the goqam file display.
Note: The “l” in ls -l is a lowercase L.
- 7 Are the access permissions for the goqam file now listed as **-rw -r - -r - -**?
 - If **yes**, you have completed this procedure.
 - If **no**, repeat this procedure once from step 4; then, if the access permissions are still incorrect, contact Cisco Services.

Verify the default configuration file

- 1 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 2 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 3 Replace the QPSK modulator if you have a spare, and contact your Cisco North American Marketing Manager to arrange for replacing or repairing the QPSK modulator.
- 4 If you cannot resolve the issues that are identified in the Doctor Report, contact Cisco Services.

QPSK Modulator Alarm ID 512 (200 Hex)

The **MAC Configuration Failure** alarm occurs when the MAC fails to configure the QPSK modulator. When this condition exists, no services are available from this QPSK modulator.

Front Panel Message

MAC config failed

Possible Cause(s)

A software error occurred when the QPSK modulator timed out while trying to complete provisioning.

Check and Correct

- 1 Manually power off and then power on the QPSK modulator, or reset the QPSK modulator from the EC.
- 2 Replace the QPSK modulator if you have a spare, and contact your Cisco North American Marketing Manager to arrange for replacing or repairing the QPSK modulator.
- 3 If the alarm continues to occur, contact Cisco Services for further assistance.

QPSK Modulator Alarm ID 515 (203 Hex)

The **DHCT Ranging Failure** alarm occurs when at least one DHCT that is already signed on to this QPSK modulator fails to range. Ranging is defined as setting power levels and timing so that messages are received properly at the QPSK demodulator. This alarm clears automatically when all DHCTs that are signed on to this QPSK modulator have successfully ranged. When this condition exists, the affected DHCTs are unable to perform interactive services.

Note: This alarm is generated only once and remains active until all DHCTs that are signed on to this QPSK modulator have successfully ranged.

Front Panel Message

Ranging Failure

Possible Cause(s)

- The most likely cause of excessive ranging failures is RF plant issues.
- The network has diminished or reduced communications capacity.
- The QPSK modulator tuner input attenuation is configured incorrectly on the EC.

Check and Correct

RF plant issues

Troubleshoot your RF plant checking signal strengths in the distribution network.

Reduced network capacity

Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.

Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.

Run the dhctStatus report on the EC.

If you cannot resolve the issues that are identified in the Doctor Report, contact Cisco Services.

Verify the QPSK modulator tuner input attenuation levels for DHCTs on the EC

Follow these steps to verify that the tuner input attenuation levels for DHCTs on the EC are identical to those required by the headend specifications.

- 1 From the EC Administrative Console, select the **EC** tab.
- 2 Select the **Element Provisioning** tab.
- 3 Select **QPSK**. The QPSK List window opens.

Chapter 5 QPSK Modulator Alarms

- 4 From the QPSK List window, double-click the QPSK modulator you are verifying. The Set Up QPSK Modulator window opens.
- 5 Select the **Advanced Parameters** tab.
- 6 In the Common Demodulator Parameters area of the window, verify that the settings in the Tuner Input Attenuation field are identical to those required in the headend specifications.
- 7 Are the tuner input attenuation parameters correct?
 - If **yes**, click **Cancel**.
 - If **no**, select the **Tuner Input Attenuation** field, and select the correct parameters from the drop down list.
- 8 Select **Save** to save the configuration.
- 9 If excessive ranging failures persist, run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 10 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report. If you cannot resolve these issues, contact Cisco Services.

QPSK Modulator Alarm ID 519 (207 Hex)

The **Invalid DAVIC Message** status event occurs when the QPSK modulator receives an invalid DAVIC message with an invalid header (the 2nd byte of DAVIC messages).

Front Panel Message

Invalid DAVIC msg

Possible Cause(s)

The QPSK modulator received an invalid DAVIC message.

Check and Correct

Invalid DAVIC message

Check all equipment that is transmitting data to the QPSK modulator.

QPSK Modulator Alarm ID 522 (20A Hex)

The **Ranging Slots at Max** status event occurs when too many DHCTs are trying to sign on to the EC at the same time.

Front Panel Message

Ranging slots at max

Possible Cause(s)

- Too many DHCTs are attempting to sign on to the EC at the same time.
- The most likely cause of excessive ranging failures is RF plant issues.
- The network has diminished or reduced communications capacity.

Check and Correct

Too many DHCTs attempting to sign on to the EC

Wait a few minutes for the DHCTs to finish signing on to the EC

RF plant issues

Troubleshoot your RF plant checking signal strengths in the distribution network.

Reduced network capacity

- 1 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 2 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 3 Run the dhctStatus utility on the EC.
- 4 If you cannot resolve the issues that are identified in the Doctor Report, contact Cisco Services.

QPSK Modulator Alarm ID 523 (20B Hex)

The **Sign On Ranging Failure** immediate status event occurs each time a DHCT fails to range when attempting to sign on. Ranging is defined as setting power levels and timing so that messages are received properly at the QPSK demodulator. When this condition exists, the affected DHCTs are unable to perform interactive services.

Important: In QPSK modulator software release versions beginning with version C64, this alarm this alarm is not set and is not sent to the EC.

Front Panel Message

None

Possible Cause(s)

The most likely cause of excessive ranging failures is RF plant issues.

The network has diminished or reduced communications capacity.

The QPSK modulator tuner input attenuation is configured incorrectly on the EC.

Check and Correct

RF plant issues

Troubleshoot your RF plant checking signal strengths in the distribution network.

Reduced network capacity

- 1 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 2 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 3 Run the dhctStatus utility on the EC
- 4 If you cannot resolve the issues that are identified in the Doctor Report, contact Cisco Services.

Chapter 5 QPSK Modulator Alarms

Accessing the dhctStatus Utility on the EC

The dhctStatus utility provides reports to help you maintain a stable network environment by quickly identifying responding and non-responding DHCTs.

Important: Refer to the *DHCT Status Reporting and signonCount Utilities User's Guide* (part number 78-738186-01) for detailed instructions on using the dhctStatus utility.

Notes:

- To complete the following instructions, the dhctStatus utility must be successfully installed on your EC.
- All UNIX commands are case-sensitive.

Follow these steps to access the dhctStatus utility on the EC.

- 1 If necessary, open an xterm window on the EC.
Note: You can be dnscs user in the xterm window.
- 2 Type **dhctStatus** and then press **Enter**. A window containing the main menu of the DHCT Status utility opens.
- 3 Troubleshoot your network using the dhctStatus utility.

QPSK Modulator Alarm ID 524 (20C Hex)

The **Connected Ranging Failure** immediate status event occurs each time a DHCT that is already signed on fails to range. Ranging is defined as setting power levels and timing so that messages are received properly at the QPSK demodulator. When this condition exists, the affected DHCTs are unable to perform interactive services.

Important! This immediate status event generates Alarm ID 515 (203 Hex) QPSK Modulator DHCT Ranging Failure.

Note: It is possible for this immediate status event to occur numerous times, but it generates the QPSK Modulator DHCT Ranging Failure alarm only on the first occurrence. The QPSK Modulator DHCT Ranging Failure alarm remains active until all DHCTs that are signed on to this QPSK modulator have successfully ranged.

Important! In QPSK modulator software release versions beginning with version C64, this alarm this alarm is not set and is not sent to the EC.

Front Panel Message

None

Possible Cause(s)

- The most likely cause of excessive ranging failures is RF plant issues.
- The network has diminished or reduced communications capacity.
- The QPSK modulator tuner input attenuation is configured incorrectly on the EC.

Check and Correct

RF plant issues

Troubleshoot your RF plant checking signal strengths in the distribution network.

Reduced network capacity

- 1 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 2 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 3 Run the dhctStatus utility on the EC.
- 4 If you cannot resolve the issues that are identified in the Doctor Report, contact Cisco Services.

QPSK Modulator Alarm ID 1024 (400 Hex)

The **Buffers Not Available** alarm occurs when the QPSK modulator is out of buffer space and is unable to allocate memory for an operation. This error will cause the QPSK modulator to automatically reboot. When this condition exists, no services are available from this QPSK modulator.

Note: This error only occurs in QPSK modulators that are running QPSK software versions prior to release A58.

Front Panel Message

Buffer not available

Possible Cause(s)

- Data overflow from IP traffic.
- Craft port activity is resulting in too many buffers being used. Using the craft port to send commands utilizes memory that the QPSK modulator needs for operation.
- There is internal software failure in the QPSK modulator.

Check and Correct

Data overflow

Check for DHCTs that are malfunctioning.

Craft port activity

Temporarily stop using the craft port. This will automatically free up buffer space.

Internal software failure

- 1 Manually power off and then power on the QPSK modulator, or reset the QPSK modulator from the EC.
- 2 If the alarm continues to occur, replace the QPSK modulator if you have a spare, and contact your Cisco North American Marketing Manager to arrange for replacing or repairing the QPSK modulator.
- 3 If the alarm continues to occur, contact Cisco Services for further assistance.

QPSK Modulator Alarm ID 1280 (500 Hex)

The **SAR Driver Initialization Failure** alarm occurs when the QPSK modulator SAR driver fails to initialize. When this condition exists, no services are available from this QPSK modulator.

The SAR process segments messages destined for Digital Home Communications Terminals (DHCTs) into ATM packets and also reassembles ATM messages from the QPSK demodulators into application messages for the QPSK modulator to process or forward.

Front Panel Message

SAR config failed

Possible Cause(s)

The SAR driver failed to initialize.

Check and Correct

- 1 Manually power off and then power on the QPSK modulator, or reset the QPSK modulator from the EC.
- 2 If the alarm continues to occur, replace the QPSK modulator if you have a spare, and contact your Cisco North American Marketing Manager to arrange for replacing or repairing the QPSK modulator.
- 3 If the alarm continues to occur, contact Cisco Services for further assistance.

QPSK Modulator Alarm ID 1284 (504 Hex)

The **SAR Receive Overflow** alarm occurs during SAR when the QPSK modulator receives an ATM AAL5 packet containing too many cells. When this condition exists, there is potential for degradation to the services from this QPSK modulator.

The SAR process segments messages destined for Digital Home Communications Terminals (DHCTs) into ATM packets and also reassembles ATM messages from the QPSK demodulators into application messages for the QPSK modulator to process or forward.

Front Panel Message

Sar rx overflow err

Possible Cause(s)

Upstream equipment is causing an overflow condition that is overwhelming the QPSK demodulator.

Check and Correct

- 1 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 2 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 3 If you cannot resolve the issues that are identified in the Doctor Report, contact Cisco Services.

QPSK Modulator Alarm ID 1285 (505 Hex)

The **SAR Buffers Full** alarm occurs when there is no free buffer space on the QPSK modulator during SAR. This error causes the QPSK modulator to reboot automatically. When this condition exists, no services are available from this QPSK modulator until after it reboots successfully.

The SAR process segments messages destined for Digital Home Communications Terminals (DHCTs) into ATM packets and also reassembles ATM messages from the QPSK demodulators into application messages for the QPSK modulator to process or forward.

Front Panel Message

Sar buffer unavailable

Possible Cause(s)

A software communication error occurred.

Check and Correct

- 1 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 2 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 3 If you cannot resolve the issues that are identified in the Doctor Report, contact Cisco Services.

QPSK Modulator Alarm ID 1286 (506 Hex)

The **SAR Timeout** alarm occurs when the QPSK modulator times out during SAR while reassembling ATM AAL5 packets. After a prolonged failure to reassemble the AAL5 packets, the QPSK modulator times out and generates an alarm.

The SAR process segments messages destined for Digital Home Communications Terminals (DHCTs) into ATM packets and also reassembles ATM messages from the QPSK demodulators into application messages for the QPSK modulator to process or forward.

Note: This alarm usually appears in conjunction with and after QPSK Modulator Alarm ID 1291 (50B Hex) **QPSK Modulator SAR CRC Error** has occurred.

When this condition exists, there is potential for degradation to the services from this QPSK modulator.

Front Panel Message

Reassembly timeout

Possible Cause(s)

Excessive reverse-path traffic is occurring on the network, and some reverse data messages are being lost.

Note: Increased repeated occurrences of this alarm usually indicate a network problem.

Check and Correct

- 1 If the majority of these alarms are happening at nearly the same time, check to see if the alarms coincide with running any of the DHCT-related reports such as non-responder or one-way status. These reports cause the DHCTs to send messages back to the EC, and consequently generate more reverse-path traffic. Reducing the rate of recurrence of such reports, or running them during off-peak hours can help alleviate this problem.
- 2 Reduce the number of DHCTs per QPSK demodulator by adding additional QPSK demodulators.
- 3 Redistribute the DHCTs on the QPSK demodulators in order to balance the load on the reverse path.
- 4 Check the distribution network for excessive noise. This could include unnecessary or unexpected applications running on the EC, the Application Server, or other components of the network.

QPSK Modulator Alarm ID 1286 (506 Hex)

- 5 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 6 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 7 If you cannot resolve the issues that are identified in the Doctor Report, contact Cisco Services.

QPSK Modulator Alarm ID 1287 (507 Hex)

The **SAR Stopped** alarm occurs during SAR when the QPSK modulator receives an invalid ATM AAL5 packet. When this condition exists, there is potential for degradation to the services from this QPSK modulator. The SAR process will restart automatically.

The SAR process segments messages destined for Digital Home Communications Terminals (DHCTs) into ATM packets and also reassembles ATM messages from the QPSK demodulators into application messages for the QPSK modulator to process or forward.

Front Panel Message

SAR Rx abort err

Possible Cause(s)

A software communication error occurred.

Check and Correct

- 1 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 2 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 3 If you cannot resolve the issues that are identified in the Doctor Report, contact Cisco Services.

QPSK Modulator Alarm ID 1288 (508 Hex)

The **SAR Multi-Buffer Error** alarm occurs during SAR on the QPSK modulator when multiple buffers exist for one ATM AAL5 packet. When this condition exists, there is potential for degradation to the services from this QPSK modulator.

The SAR process segments messages destined for Digital Home Communications Terminals (DHCTs) into ATM packets and also reassembles ATM messages from the QPSK demodulators into application messages for the QPSK modulator to process or forward.

Front Panel Message

SAR Rx multi-buffer err

Possible Cause(s)

A software communication error occurred.

Check and Correct

- 1 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 2 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 3 If you cannot resolve the issues that are identified in the Doctor Report, contact Cisco Services.

QPSK Modulator Alarm ID 1291 (50B Hex)

The **SAR CRC Error** alarm occurs on the QPSK modulator when the ATM AAL5 CRC fails during SAR. The CRC is a complex checksum protocol used to check the accuracy of the reverse-path multicell packets sent by the DHCTs back to the QPSK modulator. As the QPSK modulator attempts to reassemble the multicell packets, the CRC failure occurs due to errors in the individual packets. This can be due to an excessive amount of reverse path traffic from the DHCTs, or an excessive amount of network noise in the reverse path.

When this condition exists, there is potential for degradation to the services from this QPSK modulator.

The SAR process segments messages destined for Digital Home Communications Terminals (DHCTs) into ATM packets and also reassembles ATM messages from the QPSK demodulators into application messages for the QPSK modulator to process or forward.

Front Panel Message

SAR Rx CRC err

Possible Cause(s)

The CRC received does not match the calculated value for the message. This means that the bits in the message were received incorrectly.

Check and Correct

- 1 If the majority of these alarms are happening at nearly the same time, check to see if the alarms coincide with running any of the DHCT-related reports such as non-responder or one-way status. These reports cause the DHCTs to send messages back to the EC, and consequently generate more reverse-path traffic. Reducing the rate of recurrence of such reports, or running them during off-peak hours can help alleviate this problem.
- 2 Reduce the number of DHCTs per QPSK demodulator by adding additional QPSK demodulators.
- 3 Redistribute the DHCTs on the QPSK demodulators in order to balance the load on the reverse path.
- 4 Check the distribution network for excessive noise. This could include unnecessary or unexpected applications running on the EC, the Application Server, or other components of the network.
- 5 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 6 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 7 If you cannot resolve the issues that are identified in the Doctor Report, contact Cisco Services.

6

QPSK Demodulator Alarms

Introduction

This chapter provides detailed information for troubleshooting the alarms that are generated by the QPSK demodulator. The alarms are arranged in the ascending numeric order of the Alarm IDs. For your convenience, the Alarm IDs are listed in both decimal and hexadecimal format. You can look up the possible causes and then follow the check and correct procedures for each alarm to help you troubleshoot and clear each alarm.

Note: The actual alarm IDs sent by QPSK demodulators are large hexadecimal numbers that start with “6001.” For usability purposes, the QPSK demodulator alarms presented to users were shortened by dropping the leading numeric string “6001.” In order to derive the actual hexadecimal alarm ID that the QPSK demodulator sends, add the hexadecimal alarm ID shown to the base hexadecimal value “60010000.”

Example: For Alarm ID 1 (1 Hex), you would add the number 1 to the base hexadecimal value 60010000 to calculate the actual hexadecimal ID sent by the QPSK demodulator, which is 60010001.

QPSK Demodulator Alarm ID 0 (0 Hex)

The **Not Connected** alarm occurs when the QPSK modulator cannot communicate with a QPSK demodulator for 30 seconds or longer. There is no reverse path, and services such as PPV, IPPV, and VOD are not available from this QPSK demodulator.

Front Panel Message

Not connected

Possible Cause(s)

- A cable is loose, disconnected, or defective.
- There is no power to the QPSK demodulator.
- The QPSK demodulator has failed or is failing.

Check and Correct

Loose, disconnected, or defective cables

Check for loose connections or defective cables, tighten any loose cable connections, connect any disconnected cables, and replace any defective cables.

No power to QPSK demodulator

Check the power supply and verify that it is operational and that the unit is plugged in and powered on.

QPSK demodulator failed or failing

- 1 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 2 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 3 Replace the QPSK demodulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the QPSK demodulator.
- 4 If you cannot resolve the losses of service and the other network issues that are identified in the Doctor Report, contact Cisco Services.

QPSK Demodulator Alarm ID 1 (1 Hex)

The **ROM Flash Checksum Test Failed** alarm occurs when one of the regions in flash memory in the QPSK demodulator fails a checksum test. No services are available from this QPSK demodulator.

Front Panel Message

ROM Checksum Error

Possible Cause(s)

There is corrupt data present, or the flash memory devices in the QPSK demodulator failed.

Check and Correct

- 1 Replace the QPSK demodulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the QPSK demodulator.
- 2 If the alarm continues to occur, contact Cisco Services for further assistance.

QPSK Demodulator Alarm ID 2 (2 Hex)

The **RAM Read/Write Test Error** alarm occurs when there is a RAM read/write test error in the QPSK demodulator. No services are available from this QPSK demodulator.

Front Panel Message

RAM Test Error

Possible Cause(s)

A hardware problem occurred.

Check and Correct

- 1 Manually power off and then power on the QPSK demodulator, or reset the QPSK demodulator from the EC.
- 2 Replace the QPSK demodulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the QPSK demodulator.
- 3 If the alarm continues to occur, contact Cisco Services for further assistance.

QPSK Demodulator Alarm ID 3 (3 Hex)

The **Master I/O Device Failed** alarm occurs when the master I/O device in the QPSK demodulator is not provisioned correctly. No services are available from this QPSK demodulator.

Front Panel Message

Master I/O Error

Possible Cause(s)

Programming flash memory failed due to a hardware error, or data stored in the flash memory master I/O area in the QPSK demodulator is corrupt.

Check and Correct

- 1 Manually power off and then power on the QPSK demodulator, or reset the QPSK demodulator from the EC.
- 2 Replace the QPSK demodulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the QPSK demodulator.
- 3 If the alarm continues to occur, contact Cisco Services for further assistance.

QPSK Demodulator Alarm ID 4 (4 Hex)

The **Diagnostic Port Self-Test Failed** alarm occurs when a diagnostic port (craft port) Lbk self-test fails in the QPSK demodulator. No services are available from this QPSK demodulator.

Front Panel Message

Diag Port Lbk Error

Possible Cause(s)

The boot monitor found an error with the diagnostic port (craft port) internal loopback device.

Check and Correct

- 1 Manually power off and then power on the QPSK demodulator, or reset the QPSK demodulator from the EC.
- 2 Replace the QPSK demodulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the QPSK demodulator.
- 3 If the alarm continues to occur, contact Cisco Services for further assistance.

QPSK Demodulator Alarm ID 5 (5 Hex)

The **ATM Port Self-Test Failed** alarm occurs when the QPSK demodulator fails an ATM port self-test. No services are available from this QPSK demodulator.

Front Panel Message

ATM-25 Error

Possible Cause(s)

The boot monitor reported an error with the ATM link during initialization.

Check and Correct

- 1 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 2 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 3 Replace the QPSK demodulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the QPSK demodulator.
- 4 If you cannot resolve the issues that are identified in the Doctor Report, contact Cisco Services.

QPSK Demodulator Alarm ID 6 (6 Hex)

The **Reed-Solomon Port Self-Test Failed** alarm occurs when the QPSK demodulator fails a Reed-Solomon port self-test. Encrypted services are not available to the DHCTs served by this QPSK demodulator.

Front Panel Message

Reed-Solomon Error

Possible Cause(s)

The application reported an error with the Reed-Solomon internal loopback device.

Check and Correct

- 1 Manually power off and then power on the QPSK demodulator, or reset the QPSK demodulator from the EC.
- 2 Replace the QPSK demodulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the QPSK demodulator.
- 3 If the alarm continues to occur, contact Cisco Services for further assistance.

QPSK Demodulator Alarm ID 7 (7 Hex)

The **Burst Receiver Failed** alarm occurs when the burst receiver in the QPSK demodulator fails after provisioning and receiving burst data. There is no reverse path, and services such as PPV, IPPV, and VOD are not available from this QPSK demodulator.

Front Panel Message

Burst Rcvr Error

Possible Cause(s)

The burst receiver is not operating correctly.

Check and Correct

- 1 Manually power off and then power on the QPSK demodulator, or reset the QPSK demodulator from the EC.
- 2 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 3 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 4 Replace the QPSK demodulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the QPSK demodulator.
- 5 If you cannot resolve the issues that are identified in the Doctor Report, contact Cisco Services.

QPSK Demodulator Alarm ID 8 (8 Hex)

The **IF Burst Board Devices Not Provisioned** alarm occurs when the IF burst board programmable devices in the QPSK demodulator are not provisioned correctly. No services are available from this QPSK demodulator.

Front Panel Message

IF Burst Board Error

Possible Cause(s)

Programming flash memory failed due to a hardware error, or data stored in the flash memory IF burst board in the QPSK demodulator is corrupt.

Check and Correct

- 1 Manually power off and then power on the QPSK demodulator, or reset the QPSK demodulator from the EC.
- 2 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 3 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 4 Replace the QPSK demodulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the QPSK demodulator.
- 5 If you cannot resolve the issues that are identified in the Doctor Report, contact Cisco Services.

QPSK Demodulator Alarm ID 9 (9 Hex)

The **EEPROM Data Updated** alarm occurs when the system updates or repairs the data stored in the EEPROM in the QPSK demodulator.

Front Panel Message

Data Updated (EEPROM)

Possible Cause(s)

The system repaired corrupt data stored in EEPROM in the QPSK demodulator, or the QPSK modulator updated the data to match a new software release.

Check and Correct

Acknowledge and clear the alarm

If the alarm fails to clear, manually power off and then power on the QPSK demodulator, or reset the QPSK demodulator from the EC.

If resetting the QPSK demodulator does not solve the problem, contact Cisco Services for further assistance.

QPSK Demodulator Alarm 10 (A Hex)

The **Provisioning Data Not Received** alarm occurs when the QPSK demodulator does not receive provisioning data within 20 seconds after being powered on and cannot communicate with the qpskManager process on the EC. No services are available from this QPSK demodulator.

Note: This alarm clears automatically when communication is established with the EC and successful provisioning occurs.

Front Panel Message

Not Provisioned

Possible Cause(s)

The QPSK demodulator failed to connect to the qpskManager process on the EC.

Check and Correct

- 1 Wait at least 1 minute for the alarm to clear.
- 2 Verify that the qpskManager process is running on the EC.
- 3 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 4 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 5 If you cannot resolve the issues that are identified in the Doctor Report, contact Cisco Services.

Verifying the EC qpskManager Process

Follow these steps to verify that the EC qpskManager process is running on the EC.

- 1 In the EC Administrative Console Status window, click **Monitor** in the EC area of the window. The EC Monitor screen appears on the right of the screen.
- 2 Is the indicator to the left of qpskManager illuminated green?
 - If **yes**, the qpskManager is running. You have completed this procedure
 - If **no**, go to step 3.
- 3 From an xterm window on the EC, type dnscsControl and press Enter. The Dnscs Control window opens.
- 4 Type **2** (for Startup/Shutdown Single Element Group) and press **Enter**. The EC Startup/Shutdown Element Group selection list appears in the Dnscs Control window.
- 5 Type **3** (for QPSK Managers) and press **Enter**. The target status for element group selection list appears in the Dnscs Control window.
- 6 Type **e** (for Display Element Entries) and press **Enter**. The Startup/Shutdown Single Element Item selection list appears in the Dnscs Control window.

- 7 Type **4** (for QPSK Managers) and press **Enter**. The target status for element selection list appears in the Dncls Control window.
- 8 Press **2** (for running) and press **Enter**. A confirmation message appears.
- 9 Type **y** to confirm your entry. The EC starts the qpskManager process.
- 10 To exit, type **x** and press **Enter**.
- 11 Follow the on-screen instructions to close the Dncls Control window and to return to the xterm window.
- 12 Minimize the xterm window and look at the EC Monitor window to verify that the qpskManager process is now running.
- 13 Is the qpskManager process running?
 - If **yes**, you have completed this procedure.
 - If **no**, repeat this procedure from step 4, then go to step 14.
- 14 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 15 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 16 If you cannot resolve the issues that are identified in the Doctor Report, contact Cisco Services.

QPSK Demodulator Alarm ID 11 (B Hex)

The **Forward Path Not Synchronized** alarm occurs when the QPSK demodulator is not synchronized to the forward path. There is no reverse path, and services such as PPV, IPPV, and VOD are not available from this QPSK demodulator.

Front Panel Message

Frame Sync Error

Possible Cause(s)

The QPSK demodulator is not receiving the synchronization message from the QPSK modulator every 3 seconds.

Check and Correct

- 1 Verify that there is a correct ATM link between the QPSK demodulator and the QPSK modulator.
- 2 If the link cannot be verified, run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 3 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 4 If you cannot resolve the issues that are identified in the Doctor Report, contact Cisco Services.

QPSK Demodulator Alarm ID 12 (C Hex)

The **Reference Clock Not Functioning** alarm occurs when the reference clock in the QPSK demodulator is not functioning properly. There is severe degradation to the services from this QPSK demodulator.

Front Panel Message

No Reference Clock

Possible Cause(s)

- The encoded synchronization clock over the ATM link between the QPSK modulator and the QPSK demodulator is not occurring at the proper rate, or the synchronization clock is not present.
- The QPSK demodulator is malfunctioning.

Check and Correct

Synchronization clock malfunctioning

- 1 Verify that there is a correct ATM link between the QPSK demodulator and the QPSK modulator.
- 2 If the link cannot be verified, run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 3 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 4 Manually power down and then power up the QPSK demodulator, or reset the QPSK demodulator from the EC.
- 5 Replace the QPSK demodulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the QPSK demodulator.
- 6 If the alarm continues to occur, contact Cisco Services for further assistance.

The QPSK Demodulator is malfunctioning

- 1 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services. Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 2 Manually power off and then power on the QPSK demodulator, or reset the QPSK demodulator from the EC.
- 3 Replace the QPSK demodulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the QPSK demodulator.
- 4 If the alarm continues to occur, contact Cisco Services for further assistance.

QPSK Demodulator Alarm ID 13 (D Hex)

The **ATM Link Failed** alarm occurs when the QPSK demodulator reports poor link status to the ATM network. There is potential degradation to the reverse path affecting network communications and interactive services such as PPV, IPPV, and VOD.

Front Panel Message

Atm Link Fail

Possible Cause(s)

- The ATM connection between the QPSK demodulator and the QPSK modulator is malfunctioning.
- The QPSK demodulator is malfunctioning.

Check and Correct

ATM connection malfunctioning

- 1 Check the ATM network to verify that all cables are connected correctly and that there are no defective cables. Tighten any loose cable connections and replace any defective cables.
- 2 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 3 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 4 Manually power off and then power on the QPSK demodulator, or reset the QPSK demodulator from the EC.
- 5 If the alarm continues to occur, contact Cisco Services for further assistance.

QPSK demodulator malfunctioning

- 1 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 2 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 3 Manually power down and then power up the QPSK demodulator, or reset the QPSK demodulator from the EC.
- 4 Replace the QPSK demodulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the QPSK demodulator.
- 5 If the alarm continues to occur, contact Cisco Services for further assistance.

QPSK Demodulator Alarm ID 14 (E Hex)

The **ATM Communication Error** alarm occurs when the QPSK demodulator detects a good ATM link, however it is receiving corrupt ATM cells. There is no reverse path, and services such as PPV, IPPV, and VOD, are not available from this QPSK demodulator.

Front Panel Message

Modem Comm Error

Possible Cause(s)

The QPSK demodulator and the QPSK modulator are not communicating correctly due to AAL5 errors and ATM errors.

Check and Correct

- 1 Check the ATM network to verify that all cables are connected correctly and that there are no defective cables. Tighten any loose cable connections and replace any defective cables.
- 2 If the link cannot be verified, run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 3 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 4 Manually power off and then power on BOTH the QPSK modulator and the QPSK demodulator, or **reset** BOTH the QPSK modulator and the QPSK demodulator from the EC.
- 5 Replace the QPSK demodulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the QPSK demodulator.
- 6 If the alarm continues to occur, contact Cisco Services for further assistance.

QPSK Demodulator Alarm ID 15 (F Hex)

The **First Stage RF PLL Not Locked** alarm occurs when the first stage of the tuner RF synthesizer PLL in the QPSK demodulator is not locked. There is no reverse path, and services such as PPV, IPPV, and VOD, are not available from this QPSK demodulator.

Front Panel Message

LO1 Not Locked

Possible Cause(s)

The first stage of the tuner in the QPSK demodulator is not locked to its reference frequency.

Check and Correct

- 1 Manually power off and then power on the QPSK demodulator, or reset the QPSK demodulator from the EC.
- 2 Replace the QPSK demodulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the QPSK demodulator.
- 3 If the alarm continues to occur, contact Cisco Services for further assistance.

QPSK Demodulator Alarm ID 16 (10 Hex)

The **Second Stage RF PLL Not Locked** alarm occurs when the second stage of the tuner RF synthesizer PLL in the QPSK demodulator is not locked. There is no reverse path, and services such as PPV, IPPV, and VOD, are not available from this QPSK demodulator.

Front Panel Message

LO2 Not Locked

Possible Cause(s)

The second stage of the tuner in the QPSK demodulator is not locked to its reference frequency.

Check and Correct

- 1 Manually power off and then power on the QPSK demodulator, or reset the QPSK demodulator from the EC.
- 2 Replace the QPSK demodulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the QPSK demodulator.
- 3 If the alarm continues to occur, contact Cisco Services for further assistance.

QPSK Demodulator Alarm ID 17 (11 Hex)

The **IF PLL Not Locked** alarm occurs when the IF PLL on the QPSK demodulator is not locked to the correct reference signal. There is no reverse path, and services such as PPV, IPPV, and VOD, are not available from this QPSK demodulator.

Front Panel Message

No IF Lock

Possible Cause(s)

The IF burst board in the QPSK demodulator is not locked to its reference frequency.

Check and Correct

- 1 Manually power off and then power on the QPSK demodulator, or reset the QPSK demodulator from the EC.
- 2 Replace the QPSK demodulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the QPSK demodulator.
- 3 If the alarm continues to occur, contact Cisco Services for further assistance.

QPSK Demodulator Alarm ID 18 (12 Hex)

The **No Buffers** alarm occurs when no buffers are available in the QPSK demodulator during a 15-second interval. Only partial or intermittent reverse path is available, affecting services such as PPV, IPPV, and VOD.

Front Panel Message

Data Lost (No Buffer)

Possible Cause(s)

There is a data overload in the QPSK demodulator.

Check and Correct

- 1 Manually power off and then power on the QPSK demodulator, or reset the QPSK demodulator from the EC.
- 2 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 3 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 4 Replace the QPSK demodulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the QPSK demodulator.
- 5 If the alarm continues to occur, contact Cisco Services for further assistance.

QPSK Demodulator Alarm ID 19 (13 Hex)

The **CPU Busy** alarm occurs when the CPU in the QPSK demodulator cannot process the previous message, and/or a serial reception overrun happens within 15 seconds. Only partial or intermittent reverse path is available, affecting services such as PPV, IPPV, and VOD.

Front Panel Message

Data Lost (CPU Busy)

Possible Cause(s)

The CPU in the QPSK demodulator is receiving data faster than the device is capable of processing the data.

Check and Correct

- 1 Manually power off and then power on the QPSK demodulator, or reset the QPSK demodulator from the EC.
- 2 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 3 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 4 Replace the QPSK demodulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the QPSK demodulator.
- 5 If the alarm continues to occur, contact Cisco Services for further assistance.

QPSK Demodulator Alarm ID 20 (14 Hex)

The **Buffer Queue Full** alarm occurs when no ATM transmit or receive buffers are available in the QPSK demodulator during a 15-second interval. Only partial or intermittent reverse path is available, affecting services such as PPV, IPPV, and VOD.

Front Panel Message

Data Lost (Queue Full)

Possible Cause(s)

- The queue input and output process is unbalanced.
- There is a network overflow caused by a large number of DHCTs rebooting following a power outage.

Check and Correct

Network input/output unbalanced or network overflow

- 1 Contact your video service provider and report the problem.
- 2 Manually power off and then power on the QPSK demodulator, or reset the QPSK demodulator from the EC.
- 3 Run the Doctor Report on the EC, and examine the report for any network connectivity issues or indications of loss of services.
- 4 Troubleshoot the network connectivity issues or indications of loss of services that are identified in the Doctor Report.
- 5 Replace the QPSK demodulator if you have a spare, or contact your Cisco North American Marketing Manager to arrange for replacing or repairing the QPSK demodulator.
- 6 If the alarm continues to occur, contact Cisco Services for further assistance.

QPSK Demodulator Alarm ID 23 (17 Hex)

The **User Activity Detected** status event occurs when a user or a system operator changes the provisioning parameters on the QPSK demodulator using the front panel keys.

Front Panel Message

User Alert

Possible Cause(s)

A user or a system operator changed the provisioning parameters on the QPSK demodulator using the front panel keys.

Check and Correct

- 1 Verify what settings were changed.
- 2 Are all services functioning correctly?
 - If **yes**, no further action is required.
 - If **no**, go to step 3.
- 3 Restore the settings to the previous configuration.
- 4 Manually power off and then power on the QPSK demodulator, or reset the QPSK demodulator from the EC to restore the previous configuration.
- 5 If resetting the QPSK demodulator does not solve the problem, contact Cisco Services for further assistance.

7

Customer Information

If You Have Questions

If you have technical questions, call Cisco Services for assistance. Follow the menu options to speak with a service engineer.

Access your company's extranet site to view or order additional technical publications. For accessing instructions, contact the representative who handles your account. Check your extranet site often as the information is updated frequently.



Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA

<http://www.cisco.com>

Tel: 408 526-4000

800 553-6387

Fax: 408 527-0883

This document includes various trademarks of Cisco Systems, Inc. Please see the Notices section of this document for a list of the Cisco Systems, Inc., trademarks used in this document.

Product and service availability are subject to change without notice.

© 2014 Cisco and/or its affiliates. All rights reserved.

September 2014

Part Number OL-32771-01