Avaya Ethernet Routing Switch 2000, 3000, 4000, 5000 Series and Virtual Services Platform 7000 Series Logs Reference

NN47216-600
Issue 04.01
November 2013

© 2013 Avaya Inc.

All Rights Reserved.

Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer

“Documentation” means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya generally makes available to users of its products. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of documentation unless such modifications, additions, or deletions were performed by Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked websites referenced within this site or documentation provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Avaya provides a limited warranty on its hardware and Software (“Product(s)”). Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language, as well as information regarding support for this Product while under warranty is available to Avaya customers and other parties through the Avaya Support website: http://support.avaya.com. Please note that if you acquired the Product(s) from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by said Avaya reseller and not by Avaya. “Software” means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products or pre-installed on hardware products, and any upgrades, updates, bug fixes, or modified versions.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AUTHORIZED AVAYA RESELLER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED AVAYA RESELLER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA AUTHORIZED RESELLER; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE (“AVAYA”).

Heritage Nortel Software

“Heritage Nortel Software” means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software currently available for license from Avaya is the software contained within the list of Heritage Nortel Products located at http://support.avaya.com/LicenseInfo under the link “Heritage Nortel Products”. For Heritage Nortel Software, Avaya grants Customer a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or (in the event the applicable Documentation permits installation on non-Avaya equipment) for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, or hardware provided by Avaya. All content on this site, the documentation and the Product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Third Party Components

“Third Party Components” mean certain software programs or portions thereof included in the Software that may contain software (including open source software) distributed under third party agreements (“Third Party Components”), which contain terms regarding the rights to use certain portions of the Software (“Third Party Terms”). Information regarding distributed Linux OS source code (for those Products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the Documentation or on Avaya’s website at: http://support.avaya.com/Copyright. You agree to the Third Party Terms for any such Third Party Components.

Trademarks

The trademarks, logos and service marks (“Marks”) displayed in this site, the Documentation and Product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the Documentation and Product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners, and “Linux” is a registered trademark of Linus Torvalds.

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: http://support.avaya.com.

Contact Avaya Support

See the Avaya Support website: http://support.avaya.com for product notices and articles, or to report a problem with your Avaya product. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: http://support.avaya.com, scroll to the bottom of the page, and select Contact Avaya Support.

Contents

Chapter 1: Purpose of this document 43
Chapter 2: New in this release 45
Chapter 3: Logs fundamentals 47
Viewing system logs 47
Looking up logs in this document 47
Troubleshooting 48
Chapter 4: ADAC messages 49
ADAC warning messages 49
ADAC: ADAC of Nortel IP Phones not functional 49
ADAC: Error registering CDT handlers 49
ADAC information messages 49
ADAC Error applying main VLAN QoS configuration 49
ADAC Error applying VLAN QoS configuration for unit port unit# port# 50
ADAC Error forcing administrative state to disable enable 50
ADAC Error removing main VLAN QoS configuration 50
ADAC Error removing VLAN QoS configuration for unit port unit# port# 51
ADAC Forced administrative state to disable enable 51
ADAC System operationally disable enable 51
Chapter 5: ASCII messages 53
ASCII information messages 53
ASCII failed 53
ASCII finished successfully 53
ASCII finished successfully at load on boot 53
ASCII transfer failed 54
ASCII transfer failed at load on boot 54
ASCII transfer OK 54
ASCII transfer OK at load on boot 55
Chapter 6: AUR messages 57
AUR warning messages 57
AAUR - Warning Agent image check sum ERROR 57
AAUR - Warning Slave agent image check sum ERROR 57
DAUR - Warning Diag image check sum ERROR 57
DAUR - Warning Slave diag image check sum ERROR 58
AUR information messages 58
AAUR-Info AAUR default 58
AAUR-Info AAUR disable 58
AAUR-Info AAUR enable 58
AAUR-Info Agent transfer finished 59
AAUR-Info Receive request for agent image start transfer 59
AAUR-Info Receive request for agent image. Unable to start transfer 59
AAUR-Info Send request for new agent image 59
AAUR-Info Slave refuse transfer 60
AAUR-Info The hardware is not compatible with the image_version_number version 60
AAUR - Warning Agent image check sum ERROR 60

AAUR-Warning Cannot get FLASH resource ... 60
AAUR - Warning Slave agent image check sum ERROR ... 60
AUR-Info AUR disable ... 61
AUR-Info AUR enable ... 61
AUR-Info AUR Restored to default ... 61
AUR-Info New unit has different HW config Using cfg from the new unit ... 61
DAUR - Info Diag transfer finished ... 61
DAUR - Info Receive request for diag image start transfer ... 62
DAUR - Info Receive request for diag image. Unable to transfer ... 62
DAUR - Info Send request for new diag image ... 62
DAUR - Info Slave refuse transfer ... 62
DAUR - Info Start receive image ... 62
DAUR - The hardware is not compatible with the image_version_number version ... 63
DAUR - Warning: Cannot get FLASH resource ... 63
DAUR - Warning Diag image check sum ERROR ... 63
DAUR - Warning Slave diag image check sum ERROR ... 63
User disallowed (radius authentication fail) to log in from Web from Src IP ... 64
Chapter 7: Audit messages ... 65
Audit warning messages ... 65
Audit data initialized (bad checksum) ... 65
Audit data initialized (bad magic number) ... 65
Chapter 8: Avaya Energy Saver messages ... 67
Avaya Energy Saver information messages ... 67
Chapter 9: Bay Secure messages ... 71
Bay Secure critical messages ... 71
Bay Secure Resource Error error# line line# resource ID ... 71
Bay Secure warning messages ... 71
BaySec Not enough resource on port port# . Check QOS cfg ... 71
Bay Secure error line line# # of octets read from NVRAM ... 72
Bay Secure MAC DA filtering not enough resources ... 72
Bay Secure Policy Error error type line line# 0 ... 72
Bay Secure: Exceeded %d per-trunk MAC addresses on trunk %d ... 72
Bay Secure information messages ... 73
BaySec Exceeded number MAC addresses on unit# port# ... 73
Bay Secure Exceeded number per-port MAC addresses on port unit# port# ... 73
Bay Secure intruder ... 73
Bay Secure intruder MAC ... 74
Bay Secure per-port addresses deleted ... 74
MAC security table full ... 74
Chapter 10: CDT messages ... 75
CDT critical messages ... 75
cam driver initialization failed (code= error type argument= line#) ... 75
cam processing aborted (code= error type argument= line#) ... 75
CDT warning messages ... 76
call to cdt api function due to lock timeout (code= error type total failures= number errno= error code) ... 76
Error in XGS3 memory DMA transfer ... 76

CDT information messages ... 76
cam driver initialized ... 76
CDT MAC address mac_address was removed because LAG trunk trunked has disaggregated ... 77
CDT MAC address mac_address was removed because port port_no has aggregated in LAG ... 77
CDT The static FDB entry MAC mac_address VLAN vlan Id trunk trunkId was deleted because LAG has disaggregated ... 77
CDT The static FDB entry MAC mac_address VLAN vlan id was deleted because Unit Port unit port has aggregated ... 78
Chapter 11: CFGSO messages ... 79
CFGSO warning messages ... 79
CFGSO - Warning Invalid Msg Id ... 79
CFGSO information messages ... 79
CFGSO - Error: Failed to create watchdog timer ... 79
CFGSO - Error: Failed to get an imc buffer ... 79
CFGSO - Error: Failed to save data to NBU ... 80
CFGSO - Error: Failed to start watchdog timer ... 80
CFGSO - Error: File not read ... 80
CFGSO - Error: File not write ... 80
CFGSO - Warning Watchdog timer expire ... 80
FSH - Some files are not closed. MsgType #%d ... 81
FSH - File not closed : ... 81
Chapter 12: Config messages ... 83
Config information messages ... 83
CFG - Could not acquire FLASH sem ... 83
Chapter 13: CFM Messages ... 85
CFM Information Messages ... 85
CFM: ERROR adding port filters for VLAN %d - no resources ... 85
Chapter 14: DAI messages ... 87
DAI information messages ... 87
DAI: ARP packet with invalid IP/MAC binding dropped on untrusted port %d/%d. ARP packet has MAC source %02x-%02x-%02x-%02x-%02x-%02x ... 87
Chapter 15: DHCP Relay messages ... 89
DHCP Relay information messages ... 89
Error disabling global DHCP relay errCode ... 89
Error enabling global DHCP relay errCode ... 89
Chapter 16: DHCP Snooping messages ... 91
DHCP Snooping information messages ... 91
DHCP packet with mismatch MAC address dropped on un-trusted port unit# port# mac(MAC ADDRESS) ... 91
DHCP Snoop DHCP ACK dropped on untrusted port unit# port# (not allowed on untrusted port) ... 91
DHCP Snoop DHCP binding table is full additional DHCP clients will not be added to the binding table ... 92
DHCP Snoop DHCP NAK dropped on untrusted port unit# port# (not allowed on untrusted port) ... 92
DHCP Snoop DHCP OFFER dropped on untrusted port unit# port# (not allowed on untrusted port) 92
DHCP Snoop: DHCP packet dropped on port %d/%d - static entry with the same MAC %02x-%02x-%02x-%02x-%02x-%02x in binding table ... 93
DHCP Snoop DHCP RELEASE DECLINE dropped on untrusted port unit# port# because MAC Addr(MACaddress) is associated to port unit# port# ... 93

DHCP Snoop DHCP RELEASE DECLINE dropped on untrusted port unit# port# (MAC Addr(MACaddress) does not exist in binding table) 94
DHCP Snoop DHCP REQUEST dropped on un-trusted port unit# port# due to source MAC address(MAC ADDRESS) not matching DHCP client 94
DHCP Snoop NTP is not synchronized; external save restore of DHCP snooping entries not possible 95
DHCP Snoop DHCP snooping entry entry number not restored due to MAC conflict 95
DHCP Snoop DHCP snooping entry entry number not restored due to parsing failure 95
DHCP Snoop DHCP snooping binding table saved successfully to USB unit unit# 96
DHCP Snoop DHCP snooping entry with MAC MacAddress not restored on invalid interface unit# port# 96
DHCP Snoop DHCP snooping binding table saved successfully to TFTP address 96
DHCP Snoop DHCP snooping binding table save to USB unit unit# failed 97
DHCP Snoop DHCP snooping binding table save to TFTP address A.B.C.D IPv6_address failed. 97
DHCP Snoop DHCP snooping binding table restored successfully from USB unit unit# 97
DHCP Snoop DHCP snooping binding table restore from TFTP address A.B.C.D IPv6_address failed 97
DHCP Snoop: DHCP snooping entry 0x%08x not restored on trusted interface %d/%d 98
DHCP Snoop: DHCP snooping entry with MAC %02x-%02x-%02x-%02x-%02x-%02x not restored (invalid Vlan %d) 98
DHCP Snoop DHCP snooping binding table restore from USB unit unit# failed 98
DHCP Snoop DHCP snooping binding table restored successfully from TFTP address 99
DHCP Snoop DHCP snooping entry entry number not restored due to expired lease 99
DHCP snooping entry with MAC %02x-%02x-%02x-%02x-%02x-%02x not restored (invalid Vlan %d) 99
DHCP Snoop: DHCP snooping binding table saved successfully to SFTP address 100
DHCP Snoop: DHCP snooping binding table save to SFTP address 100
DHCP Snoop: DHCP snooping binding table succesfully restored from SFTP address 100
DHCP Snoop: DHCP snooping binding table restore from SFTP address 101
DHCP Snoop: DHCP snooping entry 0x%08x not restored on trusted interface %d/%d 101
Chapter 17: Download messages 103
Download warning messages 103
Error accessing Image File 103
Error Bad Image Checksum 103
Error reading Image File 103
Failed to Create a Watchdog 104
Failed to Read Image from Memory 104
Memory Allocation Error 104
Not Enough Memory 104
TFTP Failed 104
Memory on unit %d is under %d MBytes 105
Chapter 18: EAP messages 107
EAP information messages 107
Allowed connection attempt from user : 107
Disallowed connection Access Reject for user 107
Disallowed connection Invalid SvcType for user 107
EAP Failed qpa-RoleAssociation unitPort ifIndex macHi xx-xx macLo xx-xx-xx-xx 108
EAP GVlan Disabled for unitPort ifIndex - GVlan(vid) in different stg(id) 108
EAP Invalid RAV ID 108

EAP Invalid Vlan ID vid configured for port num ... 109
EAP Mac AuthFail - unitPort <unit-portnum> macHi <xx-xx> macLo <xx-xx-xx-xx> ... 109
EAP Unable to Reserve EapAdmin Filter Resources rc retCode unitPort ifIndex ... 109
EAP Unable to Reserve Filter Resources rc retCode unitPort ifIndex Force- Unauthorised ... 110
EAP Unable to UnReserve EapAdmin Filter Resources rc retCode unitPort ifIndex ... 110
EAP Unable to UnReserve Filter Resources rc retCode unitPort unit-portnum ... 110
EAP Failed qpa-RoleAssociation unitPort 0x%x mac %08x%04x ... 111
Got UserPolicy from Radius but UBP disabled - unitPort 0x%x mac %08x%04x ... 111
EAP CDT Error ... 111
EAP Error - Failed to free mac info memory ... 111
EAP Error - Default ... 112
EAP Failed to add host, max number of clients reached ... 112
EAP Could not process pkt ... 112
EAP Bad pkt id ... 112
EAP Bad pkt len ... 113
EAP Error while sending Access Violation Trap ... 113
EAP NULL pkt to send on Success ... 113
EAP Error while sending RAV Error Trap ... 113
EAP Vlan Change Aborted ... 114
EAP IMC Memory allocation error ... 114
EAP IMC Failed to send message ... 114
EAP Reached Mac Intruder Count ... 114
EAP Error Radius - ifIndex not found ... 115
Non-EAP Client blocked (Block Subsequent MAC Authentication): Different VID than expected ... 115
Non-EAP Client blocked (Block Subsequent MAC Authentication): EAP Use Rav Not enabled ... 115
EAP Client blocked (Block Subsequent MAC Authentication): Invalid VID ... 115
EAP Client blocked (Block Subsequent MAC Authentication): Different VID than expected ... 116
No Response from RADIUS Server ... 116
EAP Failed to add host, memory allocation error ... 116
EAP Neap port was not member of any vlan ... 116
EAP warning messages ... 117
EAP Task spawn error ... 117
EAP Failed to create dyna global arrays ... 117
EAP Message queue error ... 117
EAP Error: Reached maximum number of messages in the queue ... 117
EAP NVRAM read system admin state error ... 118
EAP NVRAM read port admin state error ... 118
EAP NVRAM read system ubp state error ... 118
EAP NVRAM open error ... 118
EAP NVRAM write error ... 119
EAP Failed initialize global arrays ... 119
NEAP Accounting - Memory allocation failure ... 119
EAP Memory allocation error ... 119
Chapter 19: Exception messages ... 121
Exception critical messages ... 121
Sw Exception ... 121
Chapter 20: Flash Driver messages ... 123

Flash Driver critical messages 123
Download - DL_CKSUM_ACK_ERROR 123
Download - DL_PROGRAM_STATUS_ACK_ERROR 123
Download - DL_START_PROGRAM_FLASH_ACK_ERROR 123
Download - Error Failed to get the dl resource 124
Download - Error Watchdog expire No Ack from NBUs download MSG # message ID 124
Download - Failed to get buffer 124
Download - Failed to malloc for buffer 124
Download - Failed to start a watchdog 125
Download - Image Checksum Error 125
Download - Largest mem blk DL_SYSMEM_RESERVED 125
Download - NBU Block Checksum Error 125
Download - NBU DL_PROGRAM_STATUS ERROR 126
Download - TFTP timeout OR image file not found 126
Download - tftpXfer failed 126
FSH - Error Calling taskLock() returns Error 126
FSH - Error Failed to erase flash sector 127
FSH - Error Failed to lock flash sector 127
FSH - Error Failed to program flash 127
FSH - Error Failed to unlock flash sector 127
FSH - Error Failed to write to flash address 128
FSH - Time to Download the Image number seconds 128
FSH - Time to Program the Image to flash number seconds 128
Reset - Error Failed to get the Reset sem 128
Flash Driver warning messages 129
Download - image type image image version programmed successfully 129
Flash Driver information messages 129
DosFs - Error File not closed 129
Chapter 21: GBIC Messages 131
GBIC Information Messages 131
Notice: DAC Cable on %s is below HW rev "H" and may cause link issues with a small number of PHYs 131
Warning:non-supported transceiver on %s has been detected 131
Info: Transceiver inserted on %s 131
Info: Transceiver removed from %s 132
SFP internal supply voltage is at high warning level on %s 132
SFP internal supply voltage is at low warning level on %s 132
SFP internal supply voltage is at high alarm level on s 132
SFP internal supply voltage is at low alarm level on %s 133
SFP internal temperature is at high alarm level on %s 133
SFP internal temperature is at low alarm level on %s 133
SFP internal temperature is at high warning level on %s 134
SFP internal temperature is at low warning level on %s 134
SFP TX Bias current is at high warning level on %s 134
SFP TX Bias current is at low warning level on %s 134
SFP TX Bias current is at low alarm level on %s 135
SFP TX Bias current is at high alarm level on %s 135
SFP TX output power is at high warning level on %s 135

SFP TX output power is at low warning level on %s ... 136
SFP TX output power is at high alarm level on %s ... 136
SFP TX output power is at low alarm level on %s ... 136
SFP Received power is at high warning level on %s ... 136
SFP Received power is at low warning level on %s ... 137
SFP Received power is at high alarm level on %s ... 137
SFP Received power is at low alarm level on %s ... 137
Chapter 22: Hello Module messages ... 139
Hello Module critical messages ... 139
Hello Module unable to communicate with neighbor(s) unit reset ... 139
Hello Module error messages ... 140
Down 1 cable removed or neighbor powered off ... 140
Down 2 cable removed or neighbor powered off ... 140
Stack cable Down 1 is misconfigured ... 140
Stack cable Down 2 is misconfigured ... 140
Up 1 cable removed or neighbor powered off ... 141
Up 2 cable removed or neighbor powered off ... 141
Stack cable Up 1 is misconfigured ... 141
Stack cable Up 2 is misconfigured ... 141
Hello Module information messages ... 142
Down 1 cable inserted or neighbor powered on ... 142
Down 2 cable inserted or neighbor powered on ... 142
Downstream stack direction is down cable removed or neighbor powered off ... 142
Downstream stack direction is mis-configured ... 142
Downstream stack direction is up cable inserted or neighbor powered on ... 143
Up 1 cable inserted or neighbor powered on ... 143
Up 2 cable inserted or neighbor powered on ... 143
Upstream stack direction is down cable removed or neighbor powered off ... 143
Upstream stack direction is mis-configured ... 144
Stack cable "Down 1" is misconfigured ... 144
Stack cable "Down 2" is misconfigured ... 144
Stack cable "Up 1" is misconfigured ... 144
Stack cable "Up 2" is misconfigured ... 145
Chapter 23: IGMP messages ... 147
IGMP critical messages ... 147
IGMP Initialization failed Error code errCode ... 147
IGMP warning messages ... 147
IGMP Error sending database from unit unit# ... 147
IGMP Error sending group database from unit unit# ... 147
IGMP information messages ... 148
IGMP Added reserved multicast address ... 148
IGMP Exceeded reserved multicast address range #Addr numResAddrEntries+1 * #VLANs numActiveVLANs maxReservedRange ... 148
IGMP Maximum number of igmp enabled interfaces reached ... 148
IGMP No hardware resource available ... 149
IGMP Proxy disabled on VLAN vlan# ... 149
IGMP Proxy enabled on VLAN vlan# ... 149

IGMP Query Time set to num on VLAN vlan# 149
IGMP Removed reserved multicast address 150
IGMP Robust Value set to num on VLAN vlan# 150
IGMP Snooping disabled on VLAN vlan# 150
IGMP Snooping enabled on VLAN vlan# 150
IGMP SSM Range changed 150
IGMP Unable to add reserved multicast address 151
IGMP Unknown Multicast Filter disabled 151
IGMP Unknown Multicast Filter enabled 151
IGMP V1 router ports mask 151
IGMP V2 router ports mask 152
IGMP: V2 report drop on reserved GA 152
IGMP: V3 report group skip on invalid GA 152
IGMP: V3 report group skip on reserved GA 152
Chapter 24: IMC messages 153
IMC critical messages 153
IMC buffers of size buffer size have been exhausted buffer pool size pool size 153
IMC warning messages 153
IMC memory allocation error packetLength = %d file %s line %d 153
IMC imc_idtPacketDispatch() incorrect rcvMsgType = %s(%d) 154
Chapter 25: IP messages 155
IP information messages 155
IPT BootP Disabled (response not received from server) 155
IPT IP Address changed by BOOTP Server 155
IPT: IP Address not in use (duplicate detected) 155
Gateway IP changed 156
Stack IP changed 156
Switch IP changed 156
Chapter 26: IPFIX messages 157
IPFIX information messages 157
IPFIX enable failure 157
Chapter 27: IPMC messages 159
IPMC warning messages 159
IGMP Maximum number of igmp enabled interfaces reached 159
IPMC information messages 159
IGMP No hardware resource available 159
IGMP SSM Range changed 160
Chapter 28: IPSG messages 161
IPSG information messages 161
Cannot disable IP Source Guard on Unit unit# Port port# 161
IP Source Guard disabled on Unit unit# Port port# 161
IP Source Guard enabled on Unit unit# Port port# 161
IPSG Insufficient resources available to enable IPSG on port unit# port# 162
IPSG nvRam file error param1 param2 param3 162
IPSG Reached Max. IP entries supported on this port port# 162
IPSG Reached Max. IP entries supported on this port unit# port# 162
IPSG Resource allocated for Ports unit# port# 163

Chapter 29: IPv6 messages 165
IPv6 information messages 165
Duplicate address deletion failed ipv6_address 165
Duplicate address detection succeeded ipv6_address 165
IPv6 enabled with hardware support and FMGR filters 166
IPv6 enabled with hardware support only 166
IPv6 malloc failure 166
IPv6 Forwarding disabled due to inadequate license 166
Chapter 30: L3 Manager messages 167
L3 Manager information messages 167
Assertion Failure in bcm_l3_hit_check- l3sw ip=%#x,l3hw ip=%#x 167
ECMP features disabled due to inadequate license 167
Failed ARP add ip addr 0xFFFFFFFF to HW hw error code 167
Failed MVLAN(vid) L3 ip addr ip mask 168
Failed to create IP intf vid ip addr in HW hw error code 168
Failed route add <ip addr/ip mask> to HW <hw error code> 168
IP blocking now 1 2 (1=ON 2=OFF) 169
Maximum number of dynamic routes reached 169
Chapter 31: LACP messages 171
LACP information messages 171
LAC MLT error on far end. 0 - 0 - 0 171
LAC No more trunk group available for LAC. 0 - 0 - 0 171
LAC: MLT error, partner aggregation bit not set 171
LAC: MLT error, partner expired bit set 172
LAC: MLT error, partner synchronization bit not set 172
LAC with admin key %d failed configuration verification. Bad VLAN configuration 172
LAC with admin key %d failed configuration verification. Bad IGMP configuration 173
LAC with admin key %d failed configuration verification. Bad rate-limiting configuration 173
LAC with admin key %d failed configuration verification. Bad DHCP-SNOOPING configuration 173
LAC with admin key %d failed configuration verification. Bad ARP INSPECTION configuration 174
LAC with admin key %d failed configuration verification. Bad MAC Security configuration 174
LAC with admin key %d failed configuration verification. Bad qos status 174
LAC with admin key %d failed configuration verification. Ports have different qos config 175
LAC with admin key %d failed configuration verification.Ports have different SPBM configurations. 175
LAC with admin key %d failed configuration verification. Error #: %d-%d 175
Chapter 32: Link State Tracking Messages 177
Link State Tracking Information Messages 177
LinkStateTracking: First interface %d/d went up in link state group %d, enabling downstream ports 177
LinkStateTracking: First interface mlt %d went up in link state group %d, enabling downstream interfaces 177
LinkStateTracking: Interface %d/d went down in link state group %d 178
LinkStateTracking: Interface %d/d went up in link state group %d 178
LinkStateTracking: Interface mlt %d went down in link state group %d 178
LinkStateTracking: Interface mlt %d went up in link state group %d 178
LinkStateTracking: Last interface %d/d went down in link state group %d, disabling downstream interfaces 179
LinkStateTracking: Last interface mlt %d went down in link state group %d, disabling downstream interfaces 179

LinkStateTracking: Interface %s went up in link state group %d ... 179
LinkStateTracking: Interface %s went up in link state group %d ... 180
LinkStateTracking: Interface %s went down in link state group %d ... 180
LinkStateTracking: Interface %s went down in link state group %d ... 180
LinkStateTracking: First interface %s went up in link state group %d, enabling downstream interfaces ... 180
LinkStateTracking: First interface %s went up in link state group %d, enabling downstream interfaces ... 181
LinkStateTracking: Last interface %s went down in link state group %d, disabling downstream interfaces ... 181
LinkStateTracking: Last interface %s went down in link state group %d, disabling downstream interfaces ... 181
Chapter 33: MLT messages ... 183
MLT information messages ... 183
MLT ID# failed configuration verification. Error # error num ... 183
MLT NV File error ... 183
MLT %d failed configuration verification. Bad VLAN configuration ... 183
MLT %d failed configuration verification. Bad VLACP configuration ... 184
MLT %d failed configuration verification. Bad IGMP configuration ... 184
MLT %d failed configuration verification. Bad rate-limiting configuration ... 184
MLT %d failed configuration verification. Bad MAC learning configuration ... 185
MLT %d failed configuration verification. Bad SPBM configuration ... 185
Last MLT trunk was allocated by MLT. No more free trunk groups ... 185
Last MLT trunk was allocated by LAC. No more free trunk groups ... 186
MLT %d failed configuration verification. Bad ARP INSPECTION configuration ... 186
MLT %d failed configuration verification. Bad DHCP-SNOOPING configuration ... 186
MLT %d failed configuration verification. Bad IPSG CLASS configuration ... 187
Chapter 34: MDA messages ... 189
MDA information messages ... 189
%s card inserted (in unit %s) ... 189
%s card removed (from unit %s) ... 189
Warning %s card unsafely removed (from unit %s) ... 189
Warning failed to connect to %s card (in unit %s) ... 190
Chapter 35: Multicast Manager Messages ... 191
Multicast Manager Critical Messages ... 191
MCM group node corrupted: ... 191
Chapter 36: MultiConfig messages ... 193
MultiConfig information messages ... 193
Backup configuration block # block_number in use ... 193
Backup configuration restored from primary configuration block # block_number ... 193
Backup configuration updated for next active configuration block # block_number ... 193
Backup Configuration Version is updated ... 194
Boot: system boot status 0x%x ... 194
Configuration saved to nv block # block_number ... 194
Error loading backup configuration block # block_number ... 194
Error loading configuration block %d ... 195
Error loading primary configuration block # block_number ... 195
Error saving configuration to block # block_number ... 195

Invalid Configuration Block Number %d ... 195
Invalid Configuration Magic Number ... 195
Invalid Configuration Version Number ... 196
Loading configuration block # block_number ... 196
Primary Configuration files are corrupted. Restored to default ... 196
Primary Configuration Version is updated ... 196
Restore Backup Configuration to Manufacture Default ... 197
Successfully loaded backup configuration files ... 197
Restore Primary Configuration to Manufacture Default ... 197
Successfully loaded configuration files from block %d ... 197
System: Rear-Port Mode has been set to disable (reboot required to take effect) ... 198
System: Rear-Port Mode has been set to enable (reboot required to take effect) ... 198
Toggle the Agent Primary Image ... 198
Configuration block %d is now in use ... 198
Successfully loaded configuration files from block %d ... 199
Successfully loaded backup configuration files ... 199
Flash Erase Warning Sector %d Address 0x%x Erase time %d ms ... 199
Flash Erase Failed Sector %d Address 0x%x ... 199
Chapter 37: NUQC messages ... 201
NUQC information messages ... 201
NUQC - Disabled ... 201
NUQC - Enabled ... 201
NUQC - Execution of the cli template failed ... 201
NUQC - Execution of the cli template succeded ... 202
Chapter 38: OSPF messages ... 203
OSPF information messages ... 203
Ospf Area Mismatch RxArea ra.rb.rc.rd IntfArea ia.ib.ic.id ... 203
Ospf Auth Failed IpAddr ia.ib.ic.id ... 203
Ospf Auto Virt Link Failed area a1.a2.a3.a4 rtid r1.r2.r3.r4 ... 203
Ospf Cost Exceeds Limit Skip route Lsid l1.l2.l3.l4 Adv-rtr a1.a2.a3.a4 ... 204
Ospf Enable Failed as Resource Unavailable ... 204
Ospf Hello: RId Same as Neighbor: rtid <r1.r2.r3.r4>, IpAddr <i1.i2.i3.i4> ... 204
Ospf HW Mode Change: ... 205
Ospf Invalid packet received: Pkt type <ospfPacketType> ... 205
Ospf License Is Missing, Disable OSPF ... 205
Ospf Nbr State Change: rtid <ra.rb.rc.rd> ipa <ia.ib.ic.id> state <neighborState> ... 205
Ospf Netmask Mismatch in Hello IpAddr ia.ib.ic.id ... 206
Ospf Option Mismatch in Hello IpAddr ia.ib.ic.id RxOption optionVal IntfOption optionVal ... 206
Ospf Virt Nbr State Change: rtid <r1.r2.r3.r4>, virtAreaId <v1.v2.v3.v4>, state <neighborState> ... 206
OspfDbg Done Global Init ... 207
OspfDbg Init Instance vrfId=%d nodeP=0x%0x ... 207
OspfDbg PostInit EnableOspf vrfId=%d nodeP=0x%0x ... 207
OspfDbg PostInit Done vrfId=%d nodeP=0x%0x ... 207
OspfDbg Started ospfTxHelloTimerTask ... 208
OspfDbg Done NV-Restore ... 208
OspfDbg Done Filter Init ... 208
OspfDbg Done ReDist Init ... 208

OSPF Callback function of timer is NULL ... 209
OSPF Timer Link Error ... 209
OSPF Timer Unlink Error ... 209
OSPF Timer List is corrupted ... 209
Ospf Bad Version ... 210
Ospf Auth Type Mismatch in Hello ... 210
Ospf Hello Int Mismatch in Hello ... 210
Ospf Dead Int Mismatch in Hello ... 210
Chapter 39: OOB Management Messages ... 211
OOB Management Serious Messages ... 211
Management IP: excess traffic received on Management port%s ... 211
OOB Management Information Messages ... 211
Management IP: OOB port%s ... 211
Management IP: OOB port%s ... 211
Chapter 40: PIM messages ... 213
PIM information messages ... 213
Pim E-BSR change ... 213
Pim Invalid packet received ... 213
Pim License Is Missing Disable PIM ... 213
Pim Mode Change ... 214
Pim Nbr State Change Up ... 214
PIM Neighbor status change Down ... 214
Pim RP type state ... 215
Pim Unicast route change ... 215
Pim Virt Nbr State Change Up ... 215
Pim Virt Nbr State Change Down ... 215
Chapter 41: PoE messages ... 217
PoE information messages ... 217
PoE Main Power Usage Off ... 217
PoE Main Power Usage On ... 217
PoE Module Reset ... 217
PoE Port Detection Status port# Status powerStatus ... 218
PoE The PoE power limit for port unit port has been changed to x Watts based on IP phone discovery settings ... 218
PoE The PoE priority for port unit port has been changed to x based on IP phone discovery settings 218
PoE The PoE power limit for port unit port has been restored to previous value x Watts ... 219
PoE The PoE priority for port unit port has been restored to previous value x ... 219
The IP phone PoE limit has been changed to x Watts due to the stack modules configuration ... 219
Chapter 42: Port Mirroring messages ... 221
Port Mirroring information messages ... 221
PM in port mirroring the old data were modified - feature Allow Traffic in mirror port was added ... 221
PM in port mirroring the old data were modified - feature Many to Many was added ... 221
PM in port mirroring the old data were modified - feature Many to One was added ... 222
PM in port mirroring the old data were modified - feature Many to One with 128bits was added ... 222
PM in port mirroring the old data were modified - mode type was out of range ... 222
PM in port mirroring the old data were modified - monitored portA was out of range ... 223
PM in port mirroring the old data were modified - monitored portB was out of range ... 223

PM in port mirroring the old data were modified - NVRAM file structure was changed..... 223
PM in port mirroring the old data were modified - probe port was out of range..... 224
PM some port mirroring messages were stored to be displayd with delay..... 224
PM unable to create mirror for instance instance number due to lack of available filter resources. 224
PM: in port mirroring the old data were modified - feature RSPAN was added..... 225
PM: instance %d has been deleted because of insufficient HW resource..... 225
Chapter 43: QoS messages..... 227
QoS critical messages..... 227
802.1p user priority mapping modifications not supported..... 227
Access assignment modifications not supported..... 227
Access element modifications not supported..... 227
Base action modifications not supported..... 228
Classifier block modifications not supported..... 228
Classifier component modifications not supported..... 228
Composite filter set addition failure comp filter set unknown..... 228
Composite filter set addition failure replication failure..... 229
Composite filter set addition failure seed filter set unknown..... 229
Composite filter set creation failure replication failure..... 229
Composite filter set creation failure seed filter set unknown..... 229
Composite filter set deletion failure comp filter set unknown..... 230
Composite filter set deletion failure seed filter set unknown..... 230
CoS shaping modifications not supported..... 230
Count action modifications not supported..... 230
Data model version attribute value not supported..... 231
DSCP mapping modifications not supported..... 231
Filter manager internal error encountered..... 231
Filter manager request parameter invalid..... 231
Incompatible data model version values (referenced clfr data)..... 232
Incompatible data model version values (referenced meter data)..... 232
Inconsistent classifier component (clfr comp#) state detected..... 232
Interface action extension identifier invalid..... 232
Interface action modifications not supported..... 233
Interface application modifications not supported..... 233
Interface assignment modifications not supported..... 233
Interface queue modifications not supported..... 233
Interface shaping modifications not supported..... 234
Invalid classifier ID specified..... 234
Invalid classifier reference (unknown class)..... 234
Invalid datapath identifier specified..... 234
Invalid master block member value specified..... 235
Invalid option specified for BcastFrames attribute..... 235
Invalid option specified for KnownIpMcast attribute..... 235
Invalid option specified for KnownMcastFrames attribute..... 235
Invalid option specified for KnownNonIpMcast attribute..... 236
Invalid option specified for KnownUcastFrames attribute..... 236
Invalid option specified for NonIpPkt attribute..... 236
Invalid option specified for UnknownMcastFrames attribute..... 236

Invalid option specified for UnknownNonIpMcast attribute..... 237
Invalid option specified for UnknownUcastFrames attribute..... 237
Invalid resetToDefaults value specified..... 237
Invalid unknown access assignment entry state encountered (entry state)..... 237
Invalid unknown access element entry state encountered (entry state)..... 238
Invalid unknown action entry state encountered (entry state)..... 238
Invalid unknown classifier block entry state encountered (entry state)..... 238
Invalid unknown CoS shaping entry state encountered (entry state)..... 238
Invalid unknown DSCP mapping entry state encountered (entry state)..... 239
Invalid unknown entry state (class class#) encountered (entry state)..... 239
Invalid unknown interface action entry state encountered (entry state)..... 239
Invalid/unknown interface app entry state encountered (<entry state>)..... 239
Invalid unknown interface assignment entry state encountered (entry state)..... 240
Invalid unknown interface queue entry state encountered (entry state)..... 240
Invalid unknown interface shaping entry state encountered (entry#)..... 240
Invalid unknown IP filter entry state encountered (entry state)..... 241
Invalid unknown Layer 2 filter entry state encountered (entry state)..... 241
Invalid unknown meter entry state encountered (entry state)..... 241
Invalid unknown policy entry state encountered (entry state)..... 241
Invalid unknown queue set assignment entry state encountered (entry state)..... 242
Invalid unknown queue shaping entry state encountered (entry state)..... 242
Invalid unknown queuing discipline enum specified (queuing discipline)..... 242
Invalid unknown role combination entry state encountered (entry state)..... 243
Invalid unknown System filter entry state encountered (entry state)..... 243
Invalid unknown token bucket entry state encountered (entry state)..... 243
Invalid unknown user policy entry state encountered (entry state)..... 243
Invalid unknown 802.1p user priority mapping entry state (entry state)..... 244
IP classifier modifications not supported..... 244
Issue detected restoring QPA data from NV (class class#)..... 244
Issues detected with QoS operational mode disable (ifcs# ifcs)..... 244
Issues detected with QoS operational mode enable (ifcs# ifcs)..... 245
Layer 2 classifier modifications not supported..... 245
Meter modifications not supported..... 245
Modify the pattern data or use the correct data format..... 245
Policy modifications not supported..... 246
Post-join policy installation issue detected (ifc ifc#)..... 246
Potential inconsistent access elem state (Undo fail) detected..... 246
Potential inconsistent block state (Undo fail) detected..... 246
Queue set assignment modifications not supported..... 247
Queue shaping modifications not supported..... 247
Resource alloc event timeout (tgt all apps except QoS Agent rcv event)..... 247
Role combination modifications not supported..... 247
Specified filter information not found..... 248
Specified filter manager resource invalid..... 248
Specified filter manager resource uninitialized..... 248
Specified policy identifier (cookie) invalid..... 248
System classifier modifications not supported..... 249

Token bucket modifications not supported ... 249
Unable to complete requested access asgn system operation (oper type) ... 249
Unable to complete requested policy system operation (operation type) ... 249
Unable to compress specified policy criteria ... 250
Unable to create action for access element ... 250
Unable to create classifier block entry for access element ... 250
Unable to create classifier component entry for access element ... 250
Unable to create DS MF classifier for access element ... 251
Unable to create L2 MF classifier for access element ... 251
Unable to install access element - component creation issue ... 251
Unable to locate corresponding DS L2 access elements ... 251
Unknown access assignment entry specified (entry#) ... 252
Unknown access element entry specified (entry#) ... 252
Unknown action entry specified (entry#) ... 252
Unknown classifier block entry specified (entry#) ... 252
Unknown classifier component entry specified (entry#) ... 253
Unknown CoS shaping entry specified (entry# CoS) ... 253
Unknown count action entry specified (entry#) ... 253
Unknown DSCP mapping entry specified (entry#) ... 253
Unknown entry (class class#) specified (entry#) ... 254
Unknown incompatible token bucket reference specified ... 254
Unknown interface application entry specified (entry#) ... 254
Unknown interface assignment entry specified (entry#) ... 254
Unknown interface queue entry specified (ifc queue id) ... 255
Unknown interface shaping entry specified (entry#) ... 255
Unknown IP classifier entry specified (entry#) ... 255
Unknown Layer 2 classifier entry specified (entry#) ... 255
Unknown meter entry specified (entry#) ... 256
Unknown policy entry specified (entry#) ... 256
Unknown queue set assignment entry specified (entry#) ... 256
Unknown queue shaping entry specified (entry# queue) ... 256
Unknown role combination entry specified (role comb id) ... 257
Unknown System classifier entry specified (entry#) ... 257
Unknown token bucket entry specified (entry#) ... 257
Unknown unsupported RowStatus specified ... 257
Unknown user policy entry specified (entry#) ... 258
Unknown 802.1p user priority mapping entry specified (entry#) ... 258
Unsupported IPv4 Options value specified ... 258
User policy modifications not supported ... 258
QoS warning messages ... 259
Access assignment modification support limited ... 259
Access assignment name contains unacceptable characters ... 259
Access assignment name length outside of acceptable limits ... 259
Access assignment name not acceptable - reserved ... 259
Access assignment template still in use (siblings active) ... 260
Access element block label contains unacceptable characters ... 260
Access element block label length outside of acceptable limits ... 260

Access element cluster count (cluster count) exceeds limit (cluster limit) 260
Access element cluster is referenced (addition prohibited) 261
Access element cluster is referenced (deletion prohibited) 261
Access element name contains unacceptable characters 261
Access element name length outside of acceptable limits 261
Access element name not acceptable - reserved 262
Attempt to create an element that already exists (prohibited) 262
Attempt to delete modify non-existing element (prohibited) 262
Attempt to manipulate system-owned interface (prohibited) 262
Attempt to manipulate user policy data rejected (disabled) 263
Base action entry referenced by clfr block (deletion prohibited) 263
Base action entry referenced by meter (deletion prohibited) 263
Base action entry referenced by policy (deletion prohibited) 263
Base action modification prohibited due to action usage 264
Base action extension identifier invalid 264
Buffer configuration inconsistency detected (local buffer conf stack buffer conf) 264
Classifier block component set ID out-of-range (clfr comp set ID) 264
Classifier block number out-of-range (block#) 265
Classifier block precedence value not supported 265
Classifier component set ID out-of-range (clfsr comp set ID) 265
Classifier conflict (duplicate clfr data in block) detected 265
Classifier content incompatible with target interface(s) 266
Classifier set block reference out-of-range (clfr setblock#) 266
Classifier type unknown 266
Clfr content (system) incompatible with target interface(s) 266
Composite filter set addition failure data consistency issue 267
Composite filter set addition failure data invalid 267
Composite filter set addition failure resources unavailable 267
Composite filter set creation failure MAC data not allowed 268
Composite filter set creation failure data invalid 268
Composite filter set deletion failure base set target invalid 268
Composite filter set deletion failure data invalid 269
Composite filter set destruction failure data invalid 269
Composite filter set membership limits exceeded 269
Conflicting action sources detected 270
Conflicting master block member information detected 270
Conflicting policy role policy interface index data detected 270
CoS shaping not supported with specified interface 270
Count action entry referenced by meter (deletion prohibited) 271
Count action entry referenced by policy (deletion prohibited) 271
DAPP resources not available (unit unit#) 271
DAPP with statistics tracking in use (QoS disable prohibited) 271
Default ifc assignment failure port# port(s) ifc QoS-disabled 272
Destination MAC address and mask values out-of-sync 272
Different classifier component masks keys in block detected 272
DSCP remarking not supported for IPv6 (green action) 272
DSCP remarking not supported for IPv6 (in-profile action) 273

DSCP remarking not supported for IPv6 (match action) 273
DSCP remarking not supported for IPv6 (non-match action) 273
DSCP remarking not supported for IPv6 (out-of-profile action) 273
DSCP remarking not supported for IPv6 (red action) 274
DSCP remarking not supported for IPv6 (yellow action) 274
Dst IP addr matching not supported with IP addr type data 274
Dst Layer 4 port min max values invalid (max must be = to min) 274
Dst MAC addr matching not supported with address type data 275
Duplicate access asgn name type index detected (prohibited) 275
Duplicate classifier class values in set detected 275
Duplicate set values in block detected 275
Egress interface and egress mask are mutually exclusive 276
Element enable prohibited. Please delete and re-enter data 276
Element label contains unacceptable characters 276
Element label length outside of acceptable limits (max 16 chars) 276
Evaluation precedence conflict (Traffic Prof filter set data) 277
Evaluation precedence conflict detected (UBP filter set data) 277
Evaluation precedence value required but not specified 277
FCoE redirection default frame filter deletion failure detected 277
FCoE redirection default frame filter installation failure detected 278
FCoE redirection - egress interface issue detected (ifIndex %d) 278
FCoE redirection - egress trunk issue detected (trunk ID %d) 278
Filter control block resources exhausted 278
Filter creation issue detected - in-profile action component 279
Filter creation issue detected - match action component 279
Filter creation issue detected - metering component 279
Filter creation issue detected - non-match action component 279
Filter creation issue detected - out-of-profile action component 280
Filter manager memory resources exhausted 280
Filter manager metering or policy rule space exhausted 280
Filter manager metering resources exhausted 280
Filter manager statistics tracking resources exhausted 281
Filter set requirements incompatible with target interface 281
First TrTCM Meter Index must be in range 1-5000 281
Flow ID filtering not supported for IPv4 281
Flow ID out-of-range (Flow ID) 282
In-profile action contains conflicting data 282
Ifc app modification issue (inconsistent default gateway data) 282
Ifc app modification issue (inconsistent DHCP server data) 282
Ifc app modification issue (inconsistent ifType data) 283
Ifc app support not currently available on interface (ifc#) 283
Ifc assignment issue - prec conflict (policy policy# disabled) 283
Inadequate resources available for application policy criteria 283
Incompatible base action extension specified 284
Incompatible classifier reference (agent-defined clfr) 284
Incompatible in-profile action (trusted ifc) 284
Incompatible in-profile action (unrestricted ifc) 284

Incompatible in-profile action (untrusted ifc)..... 285
Incompatible match action (unrestricted ifc)..... 285
Incompatible match action (untrusted ifc)..... 285
Incompatible non-match action (unrestricted ifc)..... 285
Incompatible non-match action (trusted ifc)..... 286
Incompatible non-match action (unrestricted ifc)..... 286
Incompatible non-match action (untrusted ifc)..... 286
Incompatible out-of-profile action (trusted ifc)..... 286
Incompatible out-of-profile action (unrestricted ifc)..... 287
Incompatible out-of-profile action (untrusted ifc)..... 287
Incompatible StorageType specified (re classifier)..... 287
Inconsistent action criteria detected across block members..... 287
Inconsistent labels detected for members of same block..... 288
Inconsistent labels detected for members of same set..... 288
Inconsistent MAC data detected across filter set members..... 288
Inconsistent metering criteria detected across block members..... 289
Inner VLAN ID filtering requires double tag..... 289
Inner VLAN ID min max values invalid (min VLAN ID ! max VLAN ID)..... 289
Insufficient HW resources to support port role association..... 289
Insufficient policy space available to support access assignment..... 290
Insufficient resources available to support policy installation..... 290
Interface action entry referenced by base action..... 290
Interface Application data in use (QoS disable prohibited)..... 290
Interface application Undo failure (app app#)..... 291
Interface assignment failure - precedence conflict detected..... 291
Interface capabilities incompatible with policy data..... 291
Interface resources inadequate to support application enable..... 291
Interface shaping and CoS shaping conflict (same ifc specified)..... 292
Interface shaping and queue shaping conflict (same ifc specified)..... 292
Interface shaping not supported with specified interface..... 292
Interfaces QoS-disabled (port# on unit#) - restoration issue..... 292
Invalid 802.1p user priority value specified (priority value)..... 293
Invalid access element type option specified..... 293
Invalid access assignment type option specified..... 293
Invalid classifier reference..... 293
Invalid classifier reference (unknown incompatible set)..... 294
Invalid classifier reference (unknown instance)..... 294
Interface data out-of-sync in Policy and User Policy entries..... 294
Invalid DAPP state transition detected (prohibited)..... 294
Invalid destination MAC address length specified..... 295
Invalid destination MAC address mask length specified..... 295
Invalid DSCP value specified (DSCP value)..... 295
Invalid drop precedence value specified (precedence)..... 295
Invalid egress interface specified (ifc#)..... 296
Invalid egress interface type specified (<ifc type>)..... 296
Invalid egress mask value specified..... 296
Invalid EtherType value specified (Ether Type 0xXXXX)..... 296

Invalid expired session data specified ... 297
Invalid filter set priority value detected ... 297
Invalid track statistics value specified ... 297
Invalid interface found in egress mask (egrees mask bit#) ... 297
Invalid interface index data specified (ifc#) ... 298
Invalid interface index data specified (ifc index) ... 298
Invalid interface index data (system-owned) specified ... 298
Invalid IP destination address prefix detected ... 298
Invalid IP source address prefix detected ... 299
Invalid maximum inner VLAN ID value specified (VLAN ID) ... 299
Invalid minimum inner VLAN ID value specified (VLAN ID) ... 299
Invalid maximum VLAN ID value specified (VLAN ID) ... 299
Invalid metering data (bucket size) specified for interface(s) ... 300
Invalid metering data (granularity) specified for interface(s) ... 300
Invalid metering data (rate) specified for interface(s) ... 300
Invalid metering data (srTCM trTCM) specified for interface(s) ... 300
Invalid minimum VLAN ID value specified (VLAN ID) ... 301
Invalid mix of IP address data (Dst IP type) in set detected ... 301
Invalid mix of IP data (IPv4 IPv6) in set detected ... 301
Invalid mix of IP and non-IP data in set detected ... 301
Invalid option specified for PatternIpVersion attribute ... 302
Invalid pattern data length (untagged format) specified ... 302
Invalid pattern data string length specified ... 302
Invalid pattern format data specified ... 302
Invalid pattern position string length specified ... 303
Invalid port detected in specified port mask ... 303
Invalid set drop precedence value specified ... 303
Invalid shaping data (bucket size) specified for interface(s) ... 303
Invalid shaping data (granularity) specified for interface(s) ... 304
Invalid shaping data (minimum rate granularity) specified ... 304
Invalid shaping data (minimum rate maximum rate) specified ... 304
Invalid shaping data (minimum rate) specified ... 304
Invalid shaping data (rate) specified for interface(s) ... 305
Invalid source MAC address length specified ... 305
Invalid source MAC address mask length specified ... 305
Invalid statistics counter identification specified ... 305
Invalid statistics tracking value ... 305
Invalid statistics type value ... 306
Invalid unknown bandwidth type specified ... 306
Invalid unsupported buffering capabilities value specified ... 306
Invalid unsupported copy-to-cpu option specified ... 306
Invalid unsupported DAPP enable value specified ... 307
Invalid unsupported DAPP maximum IPv4 ICMP length specified ... 307
Invalid unsupported DAPP maximum IPv6 ICMP length specified ... 307
Invalid unsupported DAPP minimum TCP header length specified ... 307
Invalid unsupported default gateway address length specified ... 308
Invalid unsupported default gateway address specified ... 308

Invalid unsupported destination IP address length specified..... 308
Invalid unsupported DHCP server address length specified..... 308
Invalid unsupported DHCP server address specified..... 309
Invalid unsupported interface type specified..... 309
Invalid unsupported mirror frame option specified..... 309
Invalid unsupported NT application mode value specified..... 309
Invalid unsupported packet type value specified..... 310
Invalid unsupported QoS system operational mode value specified..... 310
Invalid unsupported queue configuration value specified..... 310
Invalid unsupported role assoc compatibility specified..... 310
Invalid unsupported source IP address length specified..... 311
Invalid unsupported Trusted processing mode value specified..... 311
Invalid unsupported UBP support level value specified..... 311
Invalid unsupported VLAN tag value specified (VLAN tag)..... 311
Invalid update DSCP value specified (not currently supported)..... 312
Invalid update priority value specified..... 312
Invalid update VLAN Id specified (VLAN Id)..... 312
Invalid user priority match selection specified (priority value)..... 312
IPv4-only filter criteria mixed with IPv6 criteria..... 313
IP classifier entry still referenced (deletion prohibited)..... 313
IP destination address and mask values out-of-sync..... 313
IP destination Layer 4 port maximum value out-of-range (dest port#..... 313
IP destination Layer 4 port minimum value out-of-range (dest port#)..... 314
IP protocol value out-of-range (IP protocol#)..... 314
IP source address and mask values out-of-sync..... 314
IP source Layer 4 port minimum value out-of-range (src port#)..... 314
IP source Layer 4 port minimum value out-of-range (src port#)..... 315
Issue detected enabling/disabling DSCP Mapping Table usage (port %d)..... 315
Issue detected setting native DSCP Mapping Table values..... 315
Issue with classifier component mask detected..... 315
Layer 2 classifier still referenced (deletion prohibited)..... 316
Layer 4 port filtering with IPv6 requires UDP TCP Next Header..... 316
Layer 4 port range could not be reduced sufficiently..... 316
Meter (from clfr block) usage in multiple policies prohibited..... 316
Meter (from policy) usage in multiple policies prohibited..... 317
Meter entry referenced by clfr block (deletion prohibited)..... 317
Meter entry referenced by meter (deletion prohibited)..... 317
Meter entry referenced by policy (deletion prohibited)..... 317
Meter identifier out-of-range (meter id)..... 318
Metering not supported with DS L2 access control lists..... 318
Mirroring (requested via action) not configured correctly..... 318
Modification of action (non-match usage) prohibited..... 318
No resources available for classifier port range checking..... 319
Non-match action contains conflicting data..... 319
Non-match action not available for use with filter sets..... 319
Non-match action support not available on certain interfaces..... 319
Non-QoS interfaces may not be assigned to a role combination..... 320

Non-supported action option (green action) specified ... 320
Non-supported action option (in-profile action) specified ... 320
Non-supported action option (match action) specified ... 320
Non-supported action option (out-of-profile action) specified ... 321
Non-supported action option (policy non-match action) specified ... 321
Non-supported action option (red action) specified ... 321
Non-supported action option (yellow action) specified ... 321
NT application mode enable failure - inadequate resources ... 322
Non-unique precedence order value detected (prohibited) ... 322
Non-volatile QoS data discarded during restoration ... 322
Non-volatile storage commit delay too large ... 322
Only one frame type supported per classifier ... 323
Out-of-profile action contains conflicting data ... 323
Out-of-range CoS index value (COS index value) ... 323
Out-of-range queue index value (queue index) for in-use queue set ... 323
Out-of-range queue index value (queue index) for pending queue set ... 324
Packet redirection support limited by target interfaces ... 324
Pattern matching data in excess of bytes# bytes specified ... 324
Pattern matching (Dst IP) not supported with IP addr type data ... 324
Pattern matching (Dst MAC) not supported with address type data ... 325
Pattern matching (IP) not supported with non-IP addr type data ... 325
Pattern matching not supported with other classification data ... 325
Pattern modifier data specified without actual pattern data ... 325
Pattern position and data strings must be same length ... 326
Policies with session data must be port-based ... 326
Policy action out-of-range (action#) ... 326
Policy content incompatible with target interface(s) ... 326
Policy mask availability issue (space exhausted) ... 327
Policy modification support limited ... 327
Policy non-match action out-of-range (non-match action#) ... 327
Policy precedence value out-of-range for target interface(s) ... 327
Policy requirements exceed available resources (slot slot#) ... 328
Policy statistics index out-of-range (stats index) ... 328
Policy precedence conflict detected with non-QoS application ... 328
Policy with this filtering values is already installed on this precedence ... 328
Post-join ACL installation issue detected (ifc ifc#) ... 329
Post-join filter set installation issue detected (ifc ifc#) ... 329
Post-join traffic-profile installation issue detected (ifc ifc#) ... 329
Potential inconsistent access asgn state (Undo fail) detected ... 330
Potential inconsistent ifc assignment state (Undo fail) detected ... 330
Potential inconsistent policy state (Undo fail) detected ... 330
Precedence value out-of-range ... 330
Provided metering information incomplete ... 331
QoS policies may not be applied to uplink or daisy chain ports (port#) ... 331
Queue configuration inconsistency detected (local queue conf stack queue conf) ... 331
Queue set assignment distribution across stack failed ... 331
Queue set unacceptable - pending range excludes in-use queues ... 332

Queue set value modification prohibited ... 332
Rate granularity limited to increments of 1 Mbps or 64 Kbps ... 332
Rate (min) granularity limited (increments of 1 Mbps or 64 Kbps) ... 332
Referenced block (by policy) deletion prohibited ... 333
Referenced set (by block) modifications prohibited ... 333
Referenced set (by policy) modifications prohibited ... 333
Remote QoS-disable request failure (port# on unit unit#) ... 333
Request invalid - QoS interface apps enabled on interface(s) ... 334
Request invalid - specified interface currently QoS-disabled ... 334
Request temporarily denied - QoS support is currently disabled ... 334
Requested attribute usage is currently not supported ... 334
Requested filter manager support unavailable ... 335
Requested reserve data invalid ... 335
Required bandwidth information not specified ... 335
Resources exhausted (maximum class entries reached) ... 335
Resources exhausted (out-of-memory) ... 336
Role combination associated with interface (deletion prohibited) ... 336
Role combination contains unacceptable characters ... 336
Role combination referenced by policy (deletion prohibited) ... 336
Role (interface) capabilities incompatible with policy data ... 337
Source MAC address and mask values out-of-sync ... 337
Specified filter criteria is invalid inconsistent ... 337
Specified policy components (classifiers) conflicting ... 337
Specified queue set information invalid ... 338
Specified token bucket criteria out of range ... 338
Src Layer 4 port min max values invalid (max must be = to min) ... 338
srTCM meter issue - CIR must be the same in both meters ... 338
srTCM meter issue - EBS must be greater than CBS ... 339
srTCM trTCM meter issue - diff algorithms in associated meters ... 339
srTCM trTCM meter issue - referenced meter incompatible unknown ... 339
srTCM trTCM meter issue - too many cascaded meters ... 339
Specified Destination Layer 4 min max range not supported ... 340
Specified inner VLAN ID min max range not supported ... 340
Specified metering operation not supported ... 340
Specified metering statistics entry already in-use (by policy) ... 340
Specified policy components (classifiers) conflicting ... 341
Specified policy statistics entry already in-use (by meter) ... 341
Specified Source Layer 4 min max range not supported ... 341
Specified token bucket refresh interval not supported ... 341
Specified token bucket size (burst size) not supported ... 342
Specified user policy interface currently QoS-disabled ... 342
Specified VLAN ID min max range not supported ... 342
System classifier still referenced (deletion prohibited) ... 342
TCP Control Flag filter criteria requires TCP protocol ... 343
Token bucket algorithm identifier invalid ... 343
Token bucket algorithm identifier unknown unsupported ... 343
Token bucket minimum rate outside limits (64 - 10230000 Kbps) ... 343

Token bucket entry referenced by meter (deletion prohibited)..... 344
Token bucket entry referenced by shaper (deletion prohibited)..... 344
Token bucket rate outside limits (64 - 10230000 Kbps)..... 344
Token bucket size not compatible with committed fill rate..... 344
trTCM meter issue - PBS must be greater than CBS..... 345
trTCM meter issue - PIR must be greater than CIR..... 345
Traffic Prof filter set elem count exceeds available resources..... 345
Traffic Prof filter set policy count (policy count) exceeds limit (policy limit)..... 345
Traffic Prof filter set rule count (rule count) exceeds limit (rule limit)..... 346
Trusted processing mode change rejected - inadequate resources..... 346
Unable to add block member (block elem# component set id) to existing policy..... 346
Unable to apply existing policy data to interface (unit# port#)..... 346
Unable to apply existing user-based policy data to new user..... 347
Unable to apply filter set to ports (unsupported capabilities)..... 347
Unable to apply newly-defined UBP filter set to existing user..... 347
Unable to apply pre-defined UBP filter set to new user..... 347
Unable to compress classification criteria in set adequately..... 348
Unable to create out-of-profile action for access assignment..... 348
Unable to create count action (meter) for access assignment..... 348
Unable to create count action (policy) for access assignment..... 348
Unable to create count action (secondary meter) for access asgn..... 349
Unable to create metering data for access assignment..... 349
Unable to create non-match components for ACL..... 349
Unable to create token bucket data for access assignment..... 349
Unable to create policy data for access assignment..... 350
Unable to create secondary metering data for access assignment..... 350
Unable to create secondary token bucket data for access asgn..... 350
Unable to create yellow action for access assignment..... 350
Unable to deactivate policy associated with interface..... 351
Unable to delete block member (block element# component set id) from existing policy..... 351
Unable to delete UBP filter set on interface ifc#..... 351
Unable to derive suitable filter set element eval precedence..... 351
Unable to determine clfr interface(s) compatibility..... 352
Unable to disable ARP Spoofing support on interface (ifc#)..... 352
Unable to disable BPDUBlkr support on interface (ifc#)..... 352
Unable to disable DHCP Snooping support on interface (ifc#)..... 352
Unable to disable DHCP Spoofing support on interface (ifc#)..... 353
Unable to disable DNSPort support on interface (ifc#)..... 353
Unable to disable existing policy data on interface (unit# port#)..... 353
Unable to disable FTPPort support on interface (ifc#)..... 353
Unable to disable Nachia support on interface (ifc#)..... 354
Unable to disable policy data for access assignment..... 354
Unable to disable SQLSlam support on interface (ifc#)..... 354
Unable to disable SynFinScan support on interface (ifc#)..... 354
Unable to disable Xmas support on interface (ifc#)..... 355
Unable to enable ARP Spoofing support on interface (ifc#)..... 355
Unable to enable BPDUBlkr support on interface (ifc#)..... 355

Unable to enable DHCP Snooping support on interface (ifc#) ... 355
Unable to enable DHCP Spoofing support on interface (ifc#) ... 356
Unable to enable DNSPort support on interface (ifc#) ... 356
Unable to enable FTPPort support on interface (ifc#) ... 356
Unable to enable Nachia support on interface (ifc#) ... 356
Unable to enable policy data for access assignment ... 357
Unable to enable SQLSlam support on interface (ifc#) ... 357
Unable to enable SynFinScan support on interface (ifc#) ... 357
Unable to enable Xmas support on interface (ifc#) ... 357
Unable to install access assignment - component creation issue ... 358
Unable to manipulate DAPP support (no applicable interfaces) ... 358
Unable to modify access assignment - component modify issue ... 358
Unicast (Interface#) and Non-Unicast (interface#) interfaces in conflict ... 358
Unknown incompatible access element specified ... 359
Unknown incompatible action component specified ... 359
Unknown incompatible classifier block specified ... 359
Unknown incompatible classifier set specified ... 359
Unknown incompatible in-profile action specified ... 360
Unknown incompatible in-profile (green) action specified ... 360
Unknown incompatible match action specified ... 360
Unknown incompatible metering component specified ... 360
Unknown incompatible metering statistics entry specified ... 361
Unknown incompatible out-of-profile action specified ... 361
Unknown incompatible out-of-profile (red) action specified ... 361
Unknown incompatible out-of-profile (yellow) action specified ... 361
Unknown incompatible policy statistics entry specified ... 362
Unknown incompatible policy non-match action specified ... 362
Unknown incompatible queue set specified ... 362
Unknown incompatible role combination specified ... 362
Unknown incompatible token bucket reference specified ... 363
Unknown out-of-range interface index value (ifc#) ... 363
Unknown out-of-range interface index value (ifc index) ... 363
Unknown unsupported StorageType specified ... 363
Unknown unsupported interface application type specified ... 364
Unknown unsupported interface class specified (ifc class) ... 364
Unknown unsupported IP Flag specified ... 364
Unknown unsupported TCP Control Flag specified ... 364
Unknown queue set queue reference detected ... 365
Unsupported IP address type specified ... 365
Unsupported pattern offset data specified ... 365
Unsupported unknown QoS agent configuration attribute (attribute#) ... 365
Update priority value and update DSCP value out-of-sync ... 366
Update priority value per ingress DSCP currently not supported ... 366
User Policy (UBP) filter set in use (QoS disable prohibited) ... 366
User Policy (UBP) filter set in use (QoS reset prohibited) ... 366
User Policy data referencing interface (operation prohibited) ... 367
User policy filter set count (<set count>) exceeds limit (<set limit>) ... 367

User policy filter set element count exceeds available resources ... 367
User policy group contains invalid unacceptable characters ... 367
User policy group length outside of acceptable limits ... 368
User policy name contains invalid unacceptable characters ... 368
User policy name length outside of acceptable limits ... 368
User priority specified with untagged frames (invalid) ... 368
VLAN ID min max values invalid (min VLAN ID ! max VLAN ID) ... 368
VLAN range could not be reduced sufficiently ... 369
Incompatible in-profile action (untrustedv4v6 ifc) ... 369
Incompatible out-of-profile action (untrustedv4v6 ifc) ... 369
Unable to apply pre-defined UBP filter set to new user (port %d/%d) ... 369
Unable to inform SPB of ifc assignment change (%d/%d) ... 370
Incompatible match action (untrustedv4v6 ifc) ... 370
QoS information messages ... 370
802.1p user priority value modification prohibited ... 370
Access assignment distribution across stack failed ... 371
Access element distribution across stack failed ... 371
Agent configuration distribution across stack failed ... 371
Base action distribution across stack failed ... 371
Capabilities determined by agent (not-writable) ... 372
Classifier block distribution across stack failed ... 372
Classifier component distribution across stack failed ... 372
Conflicting egress interface and egress trunk data specified ... 372
COS mapping distribution across stack failed ... 373
CoS shaping distribution across stack failed ... 373
Count action distribution across stack failed ... 373
DAPP-detected DoS attack blocked unit unit# (many ports) ... 373
DAPP-detected DoS attack blocked unit unit# port port# ... 374
DAPP support disable failure ... 374
DAPP support enable failure ... 374
Data distribution class class# across stack failed ... 374
DSCP mapping distribution across stack failed ... 375
DSCP value modification prohibited ... 375
Duplicate entry detected (prohibited) ... 375
Duplicate FCoE redirection entry detected ... 375
Egress interface or trunk data is required - data missing ... 376
Element deletion prohibited (permanent read-only system entry) ... 376
Element label not acceptable - reserved ... 376
Element may only be modified not created or deleted ... 376
Element modification prohibited (read-only or system entry) ... 377
FCoE controller ifIndex not set - FCoE redirection enable prohibited ... 377
FCoE controller VLAN not set - FCoE redirection enable prohibited ... 377
Index value out-of-range ... 377
Invalid drop action option specifiedInvalid drop action option specified ... 378
Invalid entry creation attempted (index index#) ... 378
Invalid FCoE controller ingress interface specified ... 378
Invalid FCoE controller VLAN specified ... 379

Invalid/unknown FCoE redirection egress trunk ID specified 379
Invalid update DSCP value specified (DSCP value) 379
Interface action distribution across stack failed 379
Interface application distribution across stack failed 380
Interface assignment distribution across stack failed 380
IP classifier distribution across stack failed 380
IP protocol value TCP or UDP needed with Layer 4 port filtering 380
Issue detected during QoS stack synchronization 381
Issue detected enabling disabling DSCP table usage (port#) 381
Issue detected setting native DSCP table values 381
Layer 2 filter distribution across stack failed 381
Lossless and Lossless-PFC modes are only supported in queue set 2 382
Meter distribution across stack failed 382
Network access settings for FCoE Redirect must be modified locally 382
Non-unique element label detected (prohibited) 382
Policy distribution across stack failed 383
QoS inter-module communication issue detected 383
Queue data distribution across stack failed 383
Queue set value modification prohibited 383
Queue shaping distribution across stack failed 384
Role combination length outside of acceptable limits 384
Role combination distribution across stack failed 384
Simultaneous operations involving access asgn ifcs prohibited 384
Simultaneous operations involving policy blocks ifcs prohibited 385
Simultaneous operations involving policies and blocks prohibited 385
Simultaneous operations involving policies and ifcs prohibited 385
System filter distribution across stack failed 385
Token bucket data distribution across stack failed 386
Traffic Prof filter set delete operation failed 386
Traffic Prof filter set install operation failed 386
Traffic Prof filter set update operation failed 386
Unable to inform SPB of ifc assignment change (%d/%d) 387
Unknown unsupported attribute specified (attribute) 387
User policy distribution across stack failed 387
User policy filter set delete operation failed 388
User policy filter set install operation failed 388
User policy filter set update operation failed 388
Chapter 44: Quick Install messages 389
Quick Install information messages 389
QuickInstall console configuration error 389
QuickInstall:console configuration success 389
QuickInstall: Error! Unable to locate agent software file 389
QuickInstall: Error! Unable to locate ASCII configuration file 390
QuickInstall: Error! Unable to locate diagnostics software file 390
QuickInstall: Processing of USB config file has commenced 390
QuickInstall: Processing of USB config file is complete 390
QuickInstall USB config file not found 391

QuickInstall USB file config error at line line# ... 391
QuickInstall USB file config error - file exceed 200 lines ... 391
QuickInstall USB file config error - file exceed 4096 bytes ... 391
QuickInstall:USB file config success ... 392
Chapter 45: RADIUS Server Messages ... 393
Radius Server Messages ... 393
RADIUS authentication on stack serial disabled ... 393
RADIUS authentication on stack serial enabled ... 393
RADIUS authentication on stack telnet disabled ... 393
RADIUS authentication on stack telnet enabled ... 394
RADIUS authentication on switch serial disabled ... 394
RADIUS authentication on switch serial enabled ... 394
RADIUS authentication on switch telnet disabled ... 395
RADIUS authentication on switch telnet enabled ... 395
Chapter 46: RADIUS Client messages ... 397
RADIUS Client information messages ... 397
Allowed connection attempt from user ... 397
Disallowed connection Access Reject for user ... 397
Disallowed connection Invalid SvcType for user ... 397
RADIUS: ERROR - Couldn't create RADIUS Acct semaphore, errno %d ... 398
RADIUS: ERROR - Couldn't create RADIUS semaphore, errno %d ... 398
RADIUS: ERROR - Couldn't create RADIUS Acct semaphore, errno %d ... 398
RADIUS: ERROR - Couldn't start RADIUS_client() task, errno %d ... 398
RADIUS: ERROR - Couldn't start radius_recv() task, errno %d ... 399
RADIUS: ERROR - Couldn't start RADIUS_AcctClient() task, errno %d ... 399
RADIUS: ERROR - Couldn't start RADIUS_ServerCheck() task, errno %d ... 399
Chapter 47: Run Scripts messages ... 401
Run Scripts Information Messages ... 401
Error enabling IP Routing ... 401
Error configuring 802.1AB ... 401
Error configuring Management IP Address ... 401
Error configuring port names ... 402
Error configuring LLDP MED policies ... 402
Error creating Data VLAN ... 402
Error creating MLT ... 403
Error creating Voice VLAN ... 403
Error deleting previously created cost 1 default route ... 403
Error deleting previously created Voice and Data VLANs ... 404
Error enabling ADAC ... 404
Error enabling ADAC on ports ... 404
Error enabling mstp learning on all ports ... 405
Error enabling rstp learning on all ports ... 405
Error executing script ... 405
Error restoring management vlan to 1 or disabling ip routing ... 406
Error saving configuration ... 406
Error setting ADAC operating mode ... 406
Error setting call server ports ... 407

Error setting Data VLAN Gateway IP address and network mask 407
Error setting default IP Route 407
Error setting IP Office Call-Server IP address 408
Error setting IP Office File-Server IP address 408
Error setting Management VLAN 408
Error setting poe-priority high on ports 409
Error setting QoS 409
Error setting spanning-tree learning to fast on all ports 409
Error setting uplink ports 410
Error setting VLAN attributes 410
Error setting VLAN Gateway IP address and network mask 410
Error setting Voice VLAN Gateway IP address and network mask 411
Script was successfully executed 411
Voice VLAN ID and Data VLAN ID cannot have the same value 411
Chapter 48: SLPP Messages 413
SLPP Information Messages 413
SLPP-guard: hold-down timer has expired on port with SLPP-guard enabled. Port %s has been re-enabled 413
SLPP-guard: SLPP-guard has not been enabled on port %s as no filters or filter precedences are available to setup an Ethertype filter 413
SLPP-guard: SLPP packet received on port with SLPP-guard enabled. Port %s has been disabled 413
Chapter 49: SPBM Messages 415
SPBM Critical Messages 415
SPBM: ERROR adding i-sid %x to i-sid table - table full 415
SPBM: ERROR enabling SPBM due to Software License error 415
SPBM Error Messages 416
SPBM: ERROR adding C-VLAN UNI for i-sid %d, vlan %d - no resources 416
SPBM: ERROR adding i-sid %x to i-sid table - table full 416
SPBM: ERROR adding NNI on port %d vlan %d - no resources 416
SPBM: ERROR adding peer %04x.%04x.%04x - no resources 417
SPBM: ERROR adding switched UNI for i-sid %d, port %d, vlan %d - no resources 417
SPBM: ERROR adding Transparent UNI for i-sid %d, port %d - no resources 417
SPBM: ERROR updating UNI for port %d/%d - no resources 418
SPBM: ERROR adding switched UNI for i-sid %d, port %d, vlan %d - no resources 418
Chapter 50: SFTP messages 419
SFTP information messages 419
SSHC ASCII CFG download SFTP failure 419
SSHC ASCII CFG upload SFTP failure 419
SSHC CFG download SFTP failure 419
SSHC CFG upload SFTP failure 420
SSHC DSA Authentication failure 420
SSHC Password Authentication failure 420
SSHC RSA Authentication failure 420
SSHC server connection failure 421
Chapter 51: SLA Monitor messages 423
SLA Monitor Critical Messages 423
SLAMon Agent message channel creation failure 423
SLAMon Agent platform CLI command interface initialization issue 423

SLAMon Agent platform timer initialization issue ... 423
SLAMon Agent: terminated ... 424
SLAMon Agent: terminated - resources unavailable ... 424
SLAMon Agent: terminated - RTP test exception detected ... 424
SLAMon Agent: terminated - NTR test exception detected ... 424
SLAMon Agent: terminated - command/frame processing issue detected ... 424
SLAMon Agent: message channel creation failure ... 425
After agent change message became invalid: ... 425
SLA Monitor Information Messages ... 425
SLAMon Agent CLI support not available ... 425
SLAMon Agent CLI timeout value out of range ... 425
SLAMon Agent disabled ... 426
SLAMon Agent enabled ... 426
SLAMon Agent inconsistent UDP port data specified ... 426
SLAMon Agent info: %d %d %d ... 427
SLAMon Agent invalid agent-to-agent port (must be even value) ... 427
SLAMon Agent operation is restricted CLI-only ... 427
SLAMon Agent terminated ... 427
SLAMon Agent terminated — command/frame processing issue detected ... 428
SLAMon Agent terminated NTR test exception detected ... 428
SLAMon Agent terminated - resources unavailable ... 428
SLAMon Agent terminated - RTP test exception detected ... 429
Chapter 52: SMLT messages ... 431
SMLT information messages ... 431
SLPP Warning - PDU was received on Vlan VlanId Unit UnitNo Port PortNo ... 431
SMLT IMC invalid cmd 1– StkCmd ... 431
SMLT IMC tx error ... 431
SMLT input parameter error mlt port vlan ... 432
SMLT Stack db ex event num -0 –0*22221111 ... 432
SMLT stackEventNotify Invalid Msg Cmd - 0 – 0 ... 432
SMLT Stack inactive event 0-0- modMask ... 432
SMLT Stack joined event num - 0 – 0*33331111 ... 432
SMLT Stack leaved event 0 - 0 - modMask ... 433
SMLT STP enabled on IST trunk trkNo stp group grp ... 433
SMLT Warning - LAC SMLT with more than 8 links - key - count ... 433
SMLT Warning - smltEnable Software License Error- 0 – 0 ... 433
SMLT Warning - SMLT mismatched Lac_Sys_ID error shutdown all SMLT lac po ... 434
Chapter 53: SNMP Server messages ... 435
SNMP Server warning messages ... 435
Trap: FCoE - Egress Issue Detected ... 435
Trap s5CtrUnitDown ... 435
Trap: slaMonitorAgentExceptionDetected ... 435
SNMP Server information messages ... 436
Authentication Failure Trap ... 436
BPDU received on port with BPDU-Filtering enabled ... 436
Cold Start Trap ... 436
DAI ARP packet with invalid IP MAC binding dropped on untrusted port unit# port# ... 436

DHCP Snoop DHCP ACK dropped on untrusted port unit# port# (not allowed on untrusted port).. 437
DHCP Snoop DHCP binding table is full additional DHCP clients will not be added to the binding table.... 437
DHCP Snoop: DHCP DISCOVER dropped on port %d/%d (source MAC not matching client MAC) 437
DHCP Snoop DHCP NAK dropped on untrusted port unit# port# (not allowed on untrusted port).. 438
DHCP Snoop DHCP OFFER dropped on untrusted port unit# port# (not allowed on untrusted port) 438
DHCP Snoop DHCP RELEASE DECLINE dropped on untrusted port unit# port# because MAC Addr(MACaddress) is associated to port unit# port#.... 438
DHCP Snoop DHCP RELEASE DECLINE dropped on untrusted port unit# port# (MAC Addr(MACaddress) does not exist in binding table).... 439
DHCP Snoop: DHCP packet dropped on port %d/%d - static entry with the same MAC %02x-%02x-%02x-%02x-%02x-%02x in binding table.... 439
DHCP Snoop DHCP snooping binding table restored successfully from TFTP address.... 439
DHCP Snoop DHCP snooping binding table restored successfully from USB unit unit#.... 440
DHCP Snoop DHCP snooping binding table restore from TFTP address A.B.C.D IPv6_address failed.... 440
DHCP Snoop DHCP snooping binding table restore from USB unit unit# failed.... 440
DHCP Snoop DHCP snooping binding table saved successfully to TFTP address.... 440
DHCP Snoop: DHCP snooping binding table save to TFTP address, failed.... 441
DHCP Snoop DHCP snooping binding table saved successfully to USB unit unit#.... 441
DHCP Snoop DHCP snooping binding table save to USB unit unit# failed.... 441
DHCP Snoop: DHCP snooping entry with MAC %02x-%02x-%02x-%02x-%02x-%02x not restored (invalid Vlan %d).... 441
DHCP Snoop DHCP snooping entry entry number not restored due to MAC conflict.... 442
DHCP Snoop DHCP snooping entry entry number not restored due to expired lease.... 442
DHCP Snoop DHCP snooping entry with MAC MacAddress not restored on invalid interface unit# port#.... 442
DHCP Snoop DHCP snooping entry entry number not restored due to parsing failure.... 443
DHCP Snoop NTP is not synchronized; external save restore of DHCP snooping entries not possible.... 443
Egp Neighbor Loss Trap.... 443
Enterprise Specific Trap.... 443
IPSG Insufficient resources available to enable IPSG on port unit# port#.... 444
IPSG Maximum IP entries on port unit# port# has been reached.... 444
Link Down Trap.... 444
Link Up Trap.... 444
PIM Neighbor status change Up.... 445
PIM Neighbor status change Down.... 445
Radius: Server with index %d is down.... 445
Radius: Server with index %d is up.... 446
SPBM adjacency with neighbor.... 446
SPBM detect adj.... 446
SPBM ISIS.... 446
SPBM ISIS detect duplicate nick-name.... 447
SPBM ISIS node.... 447
Trap bsAdacPortConfigNotification.... 447
Trap bsAdacPortOperDisabledNotification.... 447
Trap bsnConfigurationSavedToNvram.... 448
Trap: bsDhcpSnoopingExtSaveSFTPSyncSuccess.... 448
Trap bsnEapAccessViolation.... 448

Trap bsnEapUbpFailure ... 448
Trap bsnLacPortDisabledDueToLossOfVLACPDU ... 449
Trap bsnLacPortEnabledDueToReceiptOfVLACPDU ... 449
Trap: bsnROPasswordExpired: Read-only password expired ... 449
Trap: bsnRWPasswordExpired: Read-write password expired ... 449
Trap: bsnSFPInsertion on port ... 449
Trap: bsnSFPRemoval on port ... 450
Trap bsnStackConfigurationError ... 450
Trap bsnStackManagerReconfiguration ... 450
Trap: bsnSystemUp365Days sent from unit %d ... 450
Trap bsnTrialLicenseExpiration Trial license license# has expired. Disable licensed features to avoid network interruption ... 451
Trap bsnTrialLicenseExpiration Trial license license# will expire in # days day(s) ... 451
Trap bspePethPsePortCurrentStatusNotification ... 451
Trap bsUnicastStormControlAboveHighWatermark ... 451
Trap bsUnicastStormControlBelowLowWatermark ... 452
Trap: bsnUSBInsertion on unit ... 452
Trap: bsnUSBRemoval on unit ... 452
Trap bsveVrrpTrapStateTransition ... 452
Trap DAPP - DoS Attack Detected ... 452
Trap Device has entered Forced Stack Mode (MAC Address) ... 453
Trap entConfigChange ... 453
Trap fallingAlarm ... 453
Trap lldpRemTableChange Ageouts = count ... 453
Trap lldpRemTableChange Deletes = count ... 453
Trap lldpRemTableChange Drops = count ... 454
Trap lldpRemTableChange Inserts = count ... 454
Trap lldpXMedTopologyChangeDetected Subtype = subtype Class = class ... 454
Trap newRoot ... 454
Trap ntnQosPolicyEvolLocalUbpSessionFailure ... 454
Trap ospfIfAuthFailure ... 455
Trap ospfIfConfigError ... 455
Trap ospfIfStateChange ... 455
Trap ospfNbrStateChange ... 455
Trap ospfVirtIfAuthFailure ... 455
Trap ospfVirtIfConfigError ... 456
Trap ospfVirtIfStateChange ... 456
Trap ospfVirtNbrStateChange ... 456
Trap pethMainPowerUsageOffNotification ... 456
Trap pethMainPowerUsageOnNotification ... 456
Trap pethPsePortOnOffNotification ... 457
Trap: rcIsisPlsbBvidMismatchTrap ... 457
Trap: rcIsisPlsbLsdbUpdateTrap ... 457
Trap risingAlarm ... 457
Trap RSTP Error Event ... 457
Trap RSTP General Event ... 458
Trap RSTP New Root ... 458
Trap RSTP Protocol Migration ... 458

Trap RSTP Topology Change ... 458
Trap: Run %s %s ... 458
Trap s5CtrUnitDown ... 459
Trap s5EtrSbsMacAccessViolation ... 459
Trap s5EtrSbsMacAccessViolation ... 459
Trap s5EtrSbsMacRemoved ... 459
Trap s5EtrSbsMacTableCleared ... 459
Trap s5EtrSbsMacTableClearedForPort ... 460
Trap SLPP Port Down Event ... 460
Trap Smlt Ist Link Down ... 460
Trap Smlt Ist Link Up ... 460
Trap Smlt Link Down ... 460
Trap Smlt Link Up ... 461
Trap s5CtrHotSwap ... 461
Trap topologyChange ... 461
Trap ubpEAPSessionEnd ... 461
Trap ubpEAPSessionStart ... 461
Trap vrrpTrapNewMaster ... 462
Trap: s5CtrFanDirectionError ... 462
Trap: s5CtrHighTemperatureError ... 462
Trap: s5EtrMacAddressTablesThresholdReached ... 462
Trap: rcIsisPlsbSmltVirtBmacMismatchTrap ... 463
Trap: rcIsisPlsbSmltPeerBmacMismatchTrap ... 463
Trap: rcIsisPlsbSmltSplitBebMismatchTrap ... 463
Trap: bsLstInterfaceStatusChanged ... 464
Trap: bsLstGroupOperStateChanged ... 464
Trap: bsDhcpSnoopingExtSaveSFTPSyncSuccess ... 464
Trap: bsDhcpSnoopingExtSaveSFTPSyncFailure ... 464
Trap: bsDhcpSnoopingExtSaveSFTPRestoreSuccess ... 465
Trap: bsDhcpSnoopingExtSaveSFTPRestoreFailure ... 465
DHCP Snoop: DHCP snooping entry with MAC %02x-%02x-%02x-%02x-%02x-%02x not restored on trusted interface %d/%d ... 465
Chapter 54: SNTP messages ... 467
SNTP critical messages ... 467
SNTP Could not sync to NTP servers ... 467
SNTP information messages ... 467
SNTP: First synchronization successful ... 467
Chapter 55: SSH messages ... 469
SSH information messages ... 469
SSHC: ASCII CFG download SFTP failure ... 469
SSHC: ASCII CFG upload SFTP failure ... 469
SSH_CLIENT Key couldnt be saved for host ip address ... 469
SSH CLIENT SSH Connection to IP ip address was closed because parent console session console session ID was closed ... 470
SSH CLIENT SSH Connection to %s was disconnected ... 470
SSH CLIENT: SSH Connection to %s was disconnected by host. Connection time: %s ... 470
SSH CLIENT: SSH Connection to %s was disconnected by user. Connection time: %s ... 470
SSH CLIENT Successful SSH Connection to %s using %s authentication ... 471

SSH disabled ... 471
SSH DSA key deleted ... 471
SSH DSA KEY generation completed ... 471
SSH enabled in non-secure mode ... 471
SSH enabled in secure mode ... 472
SSH Maximum number of ssh sessions has been reached ... 472
SSH RSA KEY generation completed ... 472
SSH RSA key overwritten ... 472
SSH session login using port ... 472
SSH System is generating DSA KEY wait ... 473
SSH TFTP DSA key download complete ... 473
SSH TFTP RSA key download complete ... 473
SSH USB DSA key download complete ... 473
SSH USB RSA key download complete ... 474
SSH session closed by ip address remote host. Connection time h hours m minutes ... 474
Successful SSH connection to ip address ... 474
Chapter 56: SSHC messages ... 475
SSHC information messages ... 475
SSHC: CFG download SFTP failure ... 475
SSHC: CFG upload SFTP failure ... 475
SSHC DSA key generation failure ... 476
SSHC DSA key save failure ... 476
SSHC DSA key upload TFTP failure ... 476
SSHC DSA key upload USB failure ... 476
SSHC: Password Authentication failure ... 477
SSHC: RSA Authentication failure ... 477
SSHC RSA key generation failure ... 477
SSHC RSA key save failure ... 477
SSHC RSA key upload TFTP failure ... 478
SSHC RSA key upload USB failure ... 478
Chapter 57: SSL messages ... 479
SSL information messages ... 479
SSL certificate creation completed ... 479
SSL certificate creation failed ... 479
SSL certificate deleted ... 479
SSL disabled ... 479
SSL enabled ... 480
SSL server reset ... 480
Chapter 58: Stack Manager messages ... 481
Stack Manager critical messages ... 481
application-name failed DB-exchange stack failed to form ... 481
Stack Manager warning messages ... 481
application-name failed DB-exchange stack formation delayed ... 481
Base unit has loopback port mode %s and the current unit %s. Unit reconfigured and rebooted ... 482
Different spanning-tree mode configured than BU. Unit reconfigured and rebooted ... 482
Front-panel UI selected use rear-panel base non-base switch ... 482
QOS filter-limiting mode modified and unit reset ... 483

Stack operation mode modified to Hybrid and unit reset ... 483
Stack sync failed stack failed to form ... 483
Stack synchronization failed Exp value Act value Missing value ... 483
The base (unit# number) has left the stack. Unit# number is now the base ... 484
Wrong QoS Agent queue setting, expected %u, actual %u, unit reconfigured and reboot ... 484
Wrong QoS Agent buffer setting, expected %s, actual %s, unit re-configured and reboot ... 484
Wrong QoS Agent queue setting, expected %u, actual %u, unit re-configured and reboot ... 485
Different spanning-tree mode configured than BU. Unit re-configured and rebooted ... 485
Stack Manager information messages ... 485
Another BU tried to join the stack. Unit ignored ... 485
BECOME_TEMP_BU event sent unit mask value appl mask value ... 485
Change of active config block and or reset failed block-number ... 486
DISTRIBUTE_DB event sent unit mask value appl mask value ... 486
Filter limiting mode not supported on 5510-XX unit cannot join stack ... 486
JOIN event sent unit mask value appl mask value ... 486
LEAVE event sent unit mask value appl mask value ... 487
MODULE_INACTIVE event sent unit mask value appl mask value ... 487
More than value units discovered ... 487
Multiple base units detected ... 487
Multiple Waverunner units detected when base is a Flagship ... 488
REMOVE_DATA event sent unit mask value appl mask value ... 488
Stack operation mode modified to Pure and unit reset ... 488
The BU switch is enabled. Cannot join existing stack ... 488
This unit has wrong F W version expected version actual version ... 489
This unit has wrong S W version expected version actual version ... 489
Wrong QOS Agent buffer setting expected value actual value unit cannot join stack ... 489
Stack must have a configured base unit! ... 489
Replaced "Wrong QoS Agent buffer setting, expected %u, actual %u, unit cannot join stack" with "Wrong QoS Agent buffer setting, expected %s, actual %s, unit cannot join stack" ... 490
Chapter 59: Stack Monitor messages ... 491
Stack Monitor critical messages ... 491
Task task-name is suspended ... 491
Task whose index is taskID taskID is suspended ... 491
Stack Monitor information messages ... 492
application_name failed DB-exchange stack formation delayed ... 492
Hello Module unable to communicate with neighbor(s) unit reset ... 492
IMC buffers of size size have been exhausted buffer pool size size ... 492
Stack synchronization failed stack formation delayed ... 493
Task whose index is Index1 Index2 is suspended ... 493
Task task_name is suspended ... 493
The number of stack units is number instead of expected number ... 493
Chapter 60: Source Based Routing Messages ... 495
Source Based Routing Information Messages ... 495
Topic title ... 495
IpFwdNhop Err Filter Install mod_inst=0x%08x vid=%d rv=%d ... 495
IpFwdNhop Err Filter Modify mod_inst=0x%08x vid=%d rv=%d ... 495
IpFwdNhop Err Filter UnInstall mod_inst=0x%08x vid=%d rv=%d ... 496

IpFwdNhop Err Filter UnInstall mod_inst=0x%08x vid=%d rv=%d ... 496
IpFwdNhop Err Save DB to NVRAM General File myMod=%d isBU=%d rw=%d ... 496
IpFwdNhop Err Save DB to NVRAM Instance File myMod=%d isBU=%d rw=%d ... 496
IpFwdNhop Err Save DB to NVRAM Policy File myMod=%d isBU=%d rw=%d ... 497
IpFwdNhop: Feature enable temporarily blocked - resources unavailable ... 497
IpFwdNhop: Filter installation issue - resources unavailable ... 497
IpFwdNhop: Issue detected during data restore (interface entry %d) ... 497
IpFwdNhop: Issue detected during enable retry (interface entry %d) ... 498
IpFwdNhop: Issue detected during feature enable (interface entry %d) ... 498
IpFwdNhop: Issue detected during interface creation (interface entry %d) ... 498
IpFwdNhop: Issue detected during VLAN %d routing status update ... 499
IpFwdNhop: Issue detected during VLAN membership addition (VID %d) ... 499
IpFwdNhop: Issue detected during VLAN membership deletion (VID %d) ... 499
IpFwdNhop: Issue detected during VLAN policy association (entry %d) ... 500
IpFwdNhop: Requested precedence and/or filter resources unavailable ... 500
IpFwdNhop: Requested range checking resources unavailable ... 500
IpFwdNhop: VLAN membership update (VID %d) issue - resources unavailable ... 500
Chapter 61: TACACS messages ... 503
TACACS information messages ... 503
TACACS+ accounting disabled ... 503
TACACS+ accounting enabled ... 503
TACACS authentication on stack serial disabled ... 503
TACACS authentication on stack serial enabled ... 504
TACACS+ authentication on switch serial port disabled ... 504
TACACS+ authentication on switch serial port enabled ... 504
TACACS authentication on stack telnet disabled ... 504
TACACS authentication on stack telnet enabled ... 505
TACACS+ authentication on switch telnet disabled ... 505
TACACS+ authentication on switch telnet enabled ... 505
TACACS+ authentication on switch telnet disabled ... 505
TACACS+ authentication on switch telnet enabled ... 506
TACACS+ authenticated serial connection closed ... 506
TACACS+ authenticated telnet session closed ... 506
TACACS+ authenticated telnet session max retries exceeded ... 506
TACACS authenticated SSH session closed ... 507
TACACS+ authorization disabled ... 507
TACACS+ authorization enabled ... 507
TACACS+ unsuccessful authentication ... 507
TACACS+ successful authentication ... 507
Chapter 62: Telnet messages ... 509
Telnet information messages ... 509
Connection closed. Maximum number of sessions reached. IP address: ... 509
CLI pswd: Stack auth type RADIUS/TACACS+ won't apply partially (stack IP addr not set). Local user/pass used ... 509
CLI pswd: Stack auth type RADIUS/TACACS+ won't apply partially (switch IP addr not set). Local user/pass used ... 509
Successful telnet connection to IP address ... 510
Telnet session closed by ip address remote host ... 510

TELNET: Telnet connection to IP ip address was closed because parent console session console session ID was closed ... 510
Connection closed. Maximum number of sessions reached. IP address: ... 510
Local authentication enabled on serial ... 511
Local authentication disabled on serial ... 511
Local authentication enabled on telnet ... 511
Local authentication disabled on telnet ... 511
Session opened (local auth) from IP address: ... 512
Failed login (local auth) from IP address: ... 512
Session opened (local auth) from serial connection ... 512
Failed login (local auth) from serial connection ... 512
Chapter 63: USB messages ... 513
USB information messages ... 513
USB device inserted ... 513
USB device removed ... 513
Chapter 64: Telnet Server messages ... 515
Telnet Server warning messages ... 515
Reset initiated by console ... 515
Reset initiated through SSH by IP address ... 515
Reset initiated through telnet by IP address ... 515
Reset to default initiated by console ... 516
Reset to default initiated through telnet by IP address ... 516
Stack RO password changed from IP add ... 516
Stack RO password changed from serial conn ... 516
Stack RW password changed from IP add ... 517
Stack RW password changed from serial conn ... 517
Switch RO password changed from IP add ... 517
Switch RO password changed from serial conn ... 517
Switch RW password changed from IP add ... 518
Switch RW password changed from serial conn ... 518
Telnet Server information messages ... 518
Connection closed (failed login) IP address ... 518
Connection closed (inactivity logout) IP address ... 519
Connection closed (login timeout) IP address ... 519
Connection closed (lost connection) IP address ... 519
Connection closed (user logout) IP address ... 519
Disallowed connection attempt from IP address ... 520
Disallowed connection attempt - too many telnet sessions ... 520
Failed login from IP address ... 520
Failed login from serial connection ... 520
Failed login(radius auth) from IP add ... 521
Failed login(radius auth) from serial conn ... 521
Login timeout serial connection ... 521
Session closed (inactivity logout) IP address ... 521
Session closed (inactivity logout) IP address ... 522
Session closed (lost connection) IP address ... 522
Session closed (user logout) IP address ... 522

Session closed (user logout) serial connection ... 522
Session opened from IP address ... 523
Session opened from serial connection ... 523
Session opened(radius auth) from IP add ... 523
Session opened(radius auth) from serial conn ... 523
Successful connection from IP address ... 524
Chapter 65: Unicast Storm Control messages ... 525
Unicast Storm Control information messages ... 525
Unicast unblock unit port unit_port level level watermark watermark ... 525
Unicast block unit port unit_port level level watermark watermark ... 525
USC Install SET fail unit port unit_port status = status ... 525
USC Install TEST fail unit port unit_port status = status ... 526
USC UnInst SET failed for port port status = status ... 526
Chapter 66: VLACP messages ... 527
VLACP information messages ... 527
Port %d blocked by VLACP until end-partner connection reestablished ... 527
Port %d reenabled by VLACP ... 527
Port unit# port# blocked by VLACP until end-partner connection reestablished ... 528
Port unit# port# reenabled by VLACP ... 528
Chapter 67: VLAN messages ... 529
VLAN information messages ... 529
BU was unable to send IMC for NBUs VLAN/Port configuration ... 529
Cli add vlan vlan id members port mask ... 529
Cli create vlan vlan id type port ... 529
Cli delete vlan vlan id members port mask ... 530
Cli delete vlan vlan id type port ... 530
Cli set autopvid disable ... 530
Cli set autopvid enable ... 530
Cli set management vlan vlan id ... 530
Cli set ports port mask tagging disable ... 531
Cli set ports port mask tagging enable ... 531
Cli set pvid vlan id ports port mask ... 531
Cli set vlan vlan id members port mask ... 531
Cons activate vlan vlan id ... 531
Cons add vlan vlan id port unit port ... 532
Cons create vlan vlan id type port ... 532
Cons delete vlan vlan id port unit port ... 532
Cons delete vlan vlan id type port ... 532
Cons set autopvid disable ... 532
Cons set autopvid enable ... 533
Cons set management vlan vlan id ... 533
Cons set port unit port pvid vlan id ... 533
Cons set port unit port tagging disable ... 533
Cons set port unit port tagging enable ... 533
Error getting VLAN info for Port's pvid ... 534
Error reading nvq_ObjDescr from VLAN file ... 534
Error reading prec from VLAN file ... 534

Error reading vmrec from VLAN file ... 534
Error reading vrec from VLAN file ... 535
Error restoring Ports from VLAN file ... 535
Error restoring Port from VLAN NVRAM file ... 535
Error restoring from VLAN file ... 535
Error restoring from VLAN file. Wrong nvq.Descr.devVer ... 536
Error restoring from VLAN file. Wrong nvq.Descr.notBlank ... 536
Error restoring nvq.Descr from VLAN file ... 536
Error restoring object from VLAN file - bad file pointer or mode ... 536
Error restoring object from VLAN NVRAM file ... 537
Error seeking object in VLAN file ... 537
Error restoring VLANs from VLAN file ... 537
Error restoring VMACs from VLAN file ... 537
Error seeking Ports in VLAN file ... 538
Error seeking VLANs in VLAN file ... 538
Error seeking VMACs in VLAN file ... 538
Number of VLANs does not match BU number of VLANs. VLAN config defaulted ... 538
Set port to default ... 539
VLAN configuration does not match BU VLAN configuration. VLAN config defaulted ... 539
VLAN IMC callback failed ... 539
VLAN IMC was not sent ... 540
VLAN NVRAM read error ... 540
VLAN queue messages discarded ... 540
Number of VLANs does not match BU number of VLANs. VLAN config defaulted ... 540
VLAN configuration does not match BU VLAN configuration. VLAN config defaulted ... 541
VLAN NVRAM read error ... 541
VLAN set error from IMC ... 541
VLAN set error from RPC ... 541
VLAN queue messages discarded ... 542
Wrong VLANs nvq_RecDescr actRecs ... 542
Wrong VMACs nvq_RecDescr actRecs ... 542
Wrong vrec field ... 542
Chapter 68: VRRP messages ... 545
VRRP information messages ... 545
VRRP: vrrpAdvtQueue is FULL. RX advertisement dropped in vlan %d! ... 545
VRRP: vrrpQueue is FULL. Message dropped ... 545
VRRP Feature globally disabled due to missing license ... 545
VRRP VR VR Id VLAN Id Received mismatching advertisement interval (advertisement interval) 546
VRRP VR VR Id VLAN Id Received mismatching advertisement type (advertisement type) ... 546
VRRP VR VR Id VLAN Id Received mismatching fast advertisement interval (fast advertisement interval) ... 546
VRRP VR VR Id VLAN Id Received mismatching virtual IP address (received virtual ip address) 547
VRRP VR VR Id VLAN Id Received unknown VRRP packet type (vrrp packet type) ... 547
Chapter 69: WEB messages ... 549
WEB information messages ... 549
User allowed (radius authentication pass) to log in from Web from Src IP ... 549
User disallowed (radius authentication fail) to log in from Web from Src IP ... 549

Web authentication fail from IP address..... 549
Web authentication from IP address..... 550
Web connection from IP address..... 550
Web disconnect from IP address..... 550
Web server attempting to open socket for port HTTP port..... 550
Web server starts service on port HTTP port..... 551
Web timeout from IP address..... 551

Chapter 1: Purpose of this document

Log messages record the various errors generated by the system during operation. This document is a consolidated reference of log messages generated by the system on the following platforms:

- Avaya Ethernet Routing Switch 2000 Series
- Avaya Ethernet Routing Switch 3000 Series
- Avaya Ethernet Routing Switch 4000 Series
- Avaya Ethernet Routing Switch 5000 Series
- Avaya Virtual Services Platform 7000 Series

Comments? infodev@avaya.com

Chapter 2: New in this release

The following sections describe what's new in this document.

Features

There are no new features. This document consolidates system messages for the following platforms:

- Avaya Ethernet Routing Switch 2000 Series
- Avaya Ethernet Routing Switch 3000 Series
- Avaya Ethernet Routing Switch 4000 Series
- Avaya Ethernet Routing Switch 5000 Series
- Avaya Virtual Services Platform 7000 Series

Comments? infodev@avaya.com

Chapter 3: Logs fundamentals

The following sections describe how to view, reference, and troubleshoot system logs.

Viewing system logs

You can view System logs using the ACLI.

Procedure steps

1. Log into the Privileged Exec mode.
2. Enter the **show logging** command.
3. Observe the displayed information.

Variable Definitions

Parameter	Description
Critical	Display the critical log messages.
Serious	Display the warning log messages.
Informational	Display the information log messages.

Looking up logs in this document

This document contains various log messages generated by the system, for example: ADAC, ASCII, and AUR. You can use the following two methods to find the log messages in this document:

- Browse the log messages in the bookmark and the TOC section of this guide, where they are listed in alphabetical order
- Search for log messages using the *Find* option in the Toolbar (Ctrl+F)

The log messages are included in this guide based on the following three types of severity:

- **Critical** – These messages indicate a state of crisis or emergency in the system
- **Warning** – These messages indicate a potential crisis
- **Information** – These messages display the status of the task performed on the system

Troubleshooting

If applicable, each log entry provides remedial action(s) that you can perform.

Comments? infodev@avaya.com

Chapter 4: ADAC messages

ADAC warning messages

ADAC: ADAC of Nortel IP Phones not functional

Type/Severity	Source	Description	Remedial Action
Serious	ADAC	ADAC is not working.	No action required.

ADAC: Error registering CDT handlers

Type/ Severity	Source	Description	Remedial Action
Serious	ADAC	The system detected an error when registering the CDT handlers.	No action required.

ADAC information messages

ADAC Error applying main VLAN QoS configuration

Type/Severity	Source	Description	Remedial Action
Information	ADAC	The system detected an error while applying QoS	No action required.

Type/Severity	Source	Description	Remedial Action
		or VLAN global configuration.	

ADAC Error applying VLAN QoS configuration for unit port unit# port#

Type/Severity	Source	Description	Remedial Action
Information	ADAC	The system detected an error while applying QoS or VLAN configuration from unit or port.	No action required.

ADAC Error forcing administrative state to disable enable

Type/Severity	Source	Description	Remedial Action
Information	ADAC	The system detected an error when forcing the administrative state to disable/enable.	No action required.

ADAC Error removing main VLAN QoS configuration

Type/Severity	Source	Description	Remedial Action
Information	ADAC	The system detected an error while removing QoS or VLAN global configuration.	No action required.

Comments? infodev@avaya.com

ADAC Error removing VLAN QoS configuration for unit port unit# port#

Type/Severity	Source	Description	Remedial Action
Information	ADAC	The system detected an error while removing QoS or VLAN configuration to unit or port.	No action required.

ADAC Forced administrative state to disable enable

Type/Severity	Source	Description	Remedial Action
Information	ADAC	The administrative state of ADAC feature is forced to disable/enable.	No action required.

ADAC System operationally disable enable

Type/Severity	Source	Description	Remedial Action
Information	ADAC	The system is operating with ADAC as disabled/ enabled.	No action required.

Comments? infodev@avaya.com

Chapter 5: ASCII messages

ASCII information messages

ASCII failed

Type/Severity	Source	Description	Remedial Action
Information	ACG	The ASCII configuration file contains syntax errors or inconsistent/incorrect configuration data.	Attempt to load the ASCII configuration file manually from a console and look for error messages.

ASCII finished successfully

Type/Severity	Source	Description	Remedial Action
Information	ACG	The ASCII configuration file is successfully loaded and processed during manual configuration.	No action required.

ASCII finished successfully at load on boot

Type/ Severity	Source	Description	Remedial Action
Information	ACG	The ASCII configuration file is successfully loaded and processed at boot time.	No action required.

ASCII transfer failed

Type/Severity	Source	Description	Remedial Action
Information	ACG	The ASCII configuration file could not be transferred from the TFTP server (or USB port on the switch) during manual configuration.	Check if the TFTP server is accessible. Confirm that the ASCII configuration file exists on the server (or on the USB port on the switch). Ensure that the ASCII configuration file contains appropriate permissions.

ASCII transfer failed at load on boot

Type/Severity	Source	Description	Remedial Action
Information	ACG	The ASCII configuration file could not be transferred from the TFTP server (or USB port on the switch) at boot time.	Check if the TFTP server is accessible. Confirm that the ASCII configuration file exists on the server (or on the USB port on the switch). Ensure that the ASCII configuration file contains appropriate permissions.

ASCII transfer OK

Type/Severity	Source	Description	Remedial Action
Information	ACG	The ASCII configuration file was successfully transferred from the TFTP server (or USB port on the switch) during manual configuration.	No action required.

Comments? infodev@avaya.com

ASCII transfer OK at load on boot

Type/Severity	Source	Description	Remedial Action
Information	ACG	ASCII config file was transferred successfully from TFTP server (or USB port on ERS45xx and ERS5xxx) at boot time.	No action required.

Comments? infodev@avaya.com

Chapter 6: AUR messages

AUR warning messages

AAUR - Warning Agent image check sum ERROR

Type/Severity	Source	Description	Remedial Action
Serious	AUR	Agent image check sum error.	No action required.

AAUR - Warning Slave agent image check sum ERROR

Type/Severity	Source	Description	Remedial Action
Serious	AUR	Slave agent image check sum error.	No action required.

DAUR - Warning Diag image check sum ERROR

Type/Severity	Source	Description	Remedial Action
Serious	AUR	Diag image check sum error.	No action required.

DAUR - Warning Slave diag image check sum ERROR

Type/Severity	Source	Description	Remedial Action
Serious	AUR	Slave diag image check sum error.	No action required.

AUR information messages

AAUR-Info AAUR default

Type/Severity	Source	Description	Remedial Action
Information	AUR	AAUR default.	No action required.

AAUR-Info AAUR disable

Type/Severity	Source	Description	Remedial Action
Information	AUR	The AAUR is disabled.	No action required.

AAUR-Info AAUR enable

Type/Severity	Source	Description	Remedial Action
Information	AUR	The AAUR is enabled.	No action required.

Comments? infodev@avaya.com

AAUR-Info Agent transfer finished

Type/Severity	Source	Description	Remedial Action
Information	AUR	The agent transfer is completed.	No action required.

AAUR-Info Receive request for agent image start transfer

Type/Severity	Source	Description	Remedial Action
Information	AUR	The system received request for an agent image and the transfer is started.	No action required.

AAUR-Info Receive request for agent image. Unable to start transfer

Type/Severity	Source	Description	Remedial Action
Information	AUR	The system received request for an agent image. Unable to start transfer.	No action required.

AAUR-Info Send request for new agent image

Type/Severity	Source	Description	Remedial Action
Information	AUR	The system is sending request for a new agent image.	No action required.

AAUR-Info Slave refuse transfer

Type/Severity	Source	Description	Remedial Action
Information	AUR	Slave refuse transfer.	No action required.

AAUR-Info The hardware is not compatible with the image_version_number version

Type/Severity	Source	Description	Remedial Action
Information	AUR	The hardware is not compatible.	No action required.

AAUR - Warning Agent image check sum ERROR

Type/Severity	Source	Description	Remedial Action
Serious	AUR	Agent image check sum error.	No action required.

AAUR-Warning Cannot get FLASH resource

Type/Severity	Source	Description	Remedial Action
Information	AUR	The system cannot get the flash resource.	No action required.

AAUR - Warning Slave agent image check sum ERROR

Type/Severity	Source	Description	Remedial Action
Serious	AUR	Slave agent image check sum error.	No action required.

Comments? infodev@avaya.com

AUR-Info AUR disable

Type/Severity	Source	Description	Remedial Action
Information	AUR	AUR is disabled.	No action required.

AUR-Info AUR enable

Type/Severity	Source	Description	Remedial Action
Information	AUR	AUR is enabled.	No action required.

AUR-Info AUR Restored to default

Type/Severity	Source	Description	Remedial Action
Information	AUR	AUR is restored to default.	No action required.

AUR-Info New unit has different HW config Using cfg from the new unit

Type/Severity	Source	Description	Remedial Action
Information	AUR	The new unit has a different HW configuration.	No action required.

DAUR - Info Diag transfer finished

Type/Severity	Source	Description	Remedial Action
Information	AUR	Diag transfer finished.	No action required.

DAUR - Info Receive request for diag image start transfer

Type/Severity	Source	Description	Remedial Action
Information	AUR	The system received request for the diag image and started transferring.	No action required.

DAUR - Info Receive request for diag image. Unable to transfer

Type/Severity	Source	Description	Remedial Action
Informatin	AUR	Received request for diag image, unable to start transfer.	No action required.

DAUR - Info Send request for new diag image

Type/Severity	Source	Description	Remedial Action
Information	AUR	The system is sending request for new diag image.	No action required.

DAUR - Info Slave refuse transfer

Type/Severity	Source	Description	Remedial Action
Information	AUR	Slave refuse transfer.	No action required.

DAUR - Info Start receive image

Type/Severity	Source	Description	Remedial Action
Information	AUR	The image is being received.	No action required.

Comments? infodev@avaya.com

DAUR - The hardware is not compatible with the image_version_number version

Type/Severity	Source	Description	Remedial Action
Information	AUR	The hardware is not compatible.	No action required.

DAUR - Warning: Cannot get FLASH resource

Type/Severity	Source	Description	Remedial Action
Information	AUR	The system cannot get the flash resource.	No action required.

DAUR - Warning Diag image check sum ERROR

Type/Severity	Source	Description	Remedial Action
Serious	AUR	Diag image check sum error.	No action required.

DAUR - Warning Slave diag image check sum ERROR

Type/Severity	Source	Description	Remedial Action
Serious	AUR	Slave diag image check sum error.	No action required.

User disallowed (radius authentication fail) to log in from Web from Src IP

Type/Severity	Source	Description	Remedial Action
Information	WEB	Client from the indicated IP address has failed authentication through the Radius server.	Provide the correct username and password to gain access.

Comments? infodev@avaya.com

Chapter 7: Audit messages

Audit warning messages

Audit data initialized (bad checksum)

Type/Severity	Source	Description	Remedial Action
Serious	Audit	The audit data is corrupt.	No action required.

Audit data initialized (bad magic number)

Type/Severity	Source	Description	Remedial Action
Serious	Audit	The audit data is corrupt.	No action required.

Comments? infodev@avaya.com

Chapter 8: Avaya Energy Saver messages

Avaya Energy Saver information messages

AES activated by schedule

Type/Severity	Source	Description	Remedial Action
Information	AES	The Avaya Energy Saver is activated by the AES schedule.	No action required.

AES deactivated by schedule

Type/Severity	Source	Description	Remedial Action
Information	AES	The Avaya Energy Saver is deactivated by the AES schedule.	No action required.

AES globally disabled

Type/Severity	Source	Description	Remedial Action
Information	AES	The Avaya Energy Saver is disabled.	No action required.

AES globally enabled

Type/Severity	Source	Description	Remedial Action
Information	AES	The Avaya Energy Saver is enabled.	No action required.

AES manually activated

Type/Severity	Source	Description	Remedial Action
Information	AES	The Avaya Energy Saver is manually activated.	No action required.

AES manually deactivated

Type/Severity	Source	Description	Remedial Action
Information	AES	The Avaya Energy Saver is manually deactivated.	No action required.

AES not applying schedule because SNTP not synchronized

Type/Severity	Source	Description	Remedial Action
Information	AES	The Avaya Energy Saver cannot be activated, as the internal clock is not synchronized with SNTP Server.	Check the availability of the SNTP server, and wait for the clock to be synchronized with SNTP Server.

Comments? infodev@avaya.com

AES time is synchronized applying schedule

Type/Severity	Source	Description	Remedial Action
Information	AES	The Avaya Energy Saver schedule is applied, as the clock is synchronized with the SNTP.	No action required.

Comments? infodev@avaya.com

Chapter 9: Bay Secure messages

Bay Secure critical messages

Bay Secure Resource Error error# line line# resource ID

Type/Severity	Source	Description	Remedial Action
Critical	Bay Secure	The system detected an error when operating with the task resource.	No action required.

Bay Secure warning messages

BaySec Not enough resource on port port# . Check QOS cfg

Type/Severity	Source	Description	Remedial Action
Serious	Bay Secure	The system detected an error when reserving the policy on port. (This is generated by an error in creating the Filter Manager database information for a policy and installing that policy to the hardware)	No action required.

Bay Secure error line line# # of octets read from NVRAM

Type/Severity	Source	Description	Remedial Action
Serious	Bay Secure	The system is facing problem in reading the data saved in the NVRAM.	Activate the default configuration.

Bay Secure MAC DA filtering not enough resources

Type/Severity	Source	Description	Remedial Action
Serious	Bay Secure	The system detected an error when trying to add a MAC DA filtering address. (This is generated by an error in creating the Filter Manager database information for a policy and installing that policy to the hardware)	No action required.

Bay Secure Policy Error error type line line# 0

Type/Severity	Source	Description	Remedial Action
Serious	Bay Secure	The system detected an error in getting or setting a policy.	No action required.

Bay Secure: Exceeded %d per-trunk MAC addresses on trunk %d

Type/Severity	Source	Description	Remedial Action
Warning/ Information	DHCPSNOOP	This notification is generated after successfully saving the DHCP snooping binding	No action required.

Comments? infodev@avaya.com

Type/Severity	Source	Description	Remedial Action
		table to a SFTP server external file.	

Bay Secure information messages

BaySec Exceeded number MAC addresses on unit# port#

Type/Severity	Source	Description	Remedial Action
Information	Bay Secure	This message appears when the system is trying to set too many security roles on a port.	No action required.

Bay Secure Exceeded number per-port MAC addresses on port unit# port#

Type/Severity	Source	Description	Remedial Action
Information	Bay Secure	The maximum number of MAC addresses that can be learned on a port is reached.	No action required.

Bay Secure intruder

Type/Severity	Source	Description	Remedial Action
Information	Bay Secure	The system detected an intruder.	No action required.

Bay Secure intruder MAC

Type/Severity	Source	Description	Remedial Action
Information	Bay Secure	The system detected an intruder.	No action required.

Bay Secure per-port addresses deleted

Type/Severity	Source	Description	Remedial Action
Information	Bay Secure	An auto-learned address is deleted (This warning appears only on the BU or stand-alone switch).	No action required.

MAC security table full

Type/Severity	Source	Description	Remedial Action
Information	Bay secure	The MAC security table is full.	No action required.

Comments? infodev@avaya.com

Chapter 10: CDT messages

CDT critical messages

cam driver initialization failed (code= error type argument= line#)

Type/Severity	Source	Description	Remedial Action
Critical	CDT	The CAM driver initialization critically failed, as the system resources were unavailable.	Restart the system.

cam processing aborted (code= error type argument= line#)

Type/Severity	Source	Description	Remedial Action
Critical	CDT	The system could not process the MAC address, due to repeated internal failures.	No action required.

CDT warning messages

call to cdt api function due to lock timeout (code= error type total failures= number errno= error code)

Type/Severity	Source	Description	Remedial Action
Serious	CDT	The system detected an error caused by failure in the mutual exclusion lock mechanisms.	No action required.

Error in XGS3 memory DMA transfer

Type/Severity	Source	Description	Remedial Action
Serious	CDT	Logs an error for XGS3 switches in case of DMA error.	Reboot device

CDT information messages

cam driver initialized

Type/Severity	Source	Description	Remedial Action
Information	CDT	The system initialized the CAM driver.	No action required.

Comments? infodev@avaya.com

CDT MAC address mac_address was removed because LAG trunk trunked has disaggregated.

Type/Severity	Source	Description	Remedial Action
Information	CDT	The static MAC address for a LAG trunk was deleted because the specific LAG trunk is disaggregated.	No action required.

CDT MAC address mac_address was removed because port port_no has aggregated in LAG

Type/Severity	Source	Description	Remedial Action
Information	CDT	The static MAC address for a port is deleted, because the specific port is aggregated in a LAG	No action required.

CDT The static FDB entry MAC mac_address VLAN vlan Id trunk trunkId was deleted because LAG has disaggregated

Type/Severity	Source	Description	Remedial Action
Information	CDT	The static MAC address for a LAG trunk was deleted because the specific LAG trunk has disaggregated.	No action required.

CDT The static FDB entry MAC mac_address VLAN vlan id was deleted because Unit Port unit port has aggregated

Type/Severity	Source	Description	Remedial Action
Information	CDT	The static MAC address for a port was deleted as the specific port has aggregated in a LAG.	No action required.

Comments? infodev@avaya.com

Chapter 11: CFGSO messages

CFGSO warning messages

CFGSO - Warning Invalid Msg Id

Type/Severity	Source	Description	Remedial Action
Serious	CFGSO	The system detected an invalid message Id.	No action required.

CFGSO information messages

CFGSO - Error: Failed to create watchdog timer

Type/Severity	Source	Description	Remedial Action
Information	CFGSO	The system failed to create a watchdog timer.	No action required.

CFGSO - Error: Failed to get an imc buffer

Type/Severity	Source	Description	Remedial Action
Information	CFGSO	The system failed to get an IMC buffer.	No action required.

CFGSO - Error: Failed to save data to NBU

Type/Severity	Source	Description	Remedial Action
Information	CFGSO	The system failed to save data to NBU.	No action required.

CFGSO - Error: Failed to start watchdog timer

Type/Severity	Source	Description	Remedial Action
Information	CFGSO	The system failed to start the watchdog timer.	No action required.

CFGSO - Error: File not read

Type/Severity	Source	Description	Remedial Action
Information	CFGSO	The system could not read the file.	No action required.

CFGSO - Error: File not write

Type/Severity	Source	Description	Remedial Action
Information	CFGSO	The system could not write the file.	No action required.

CFGSO - Warning Watchdog timer expire

Type/Severity	Source	Description	Remedial Action
Error	CFGSO	The watchdog timer expired.	No action required.

Comments? infodev@avaya.com

FSH - Some files are not closed. MsgType #%d

Type/Severity	Source	Description	Remedial Action
Information	CFC	This notification is generated while trying to load/save the configuration, if some files remain open. The configuration cannot be saved if the files remain open.	No action required.

FSH - File not closed :

Type/Severity	Source	Description	Remedial Action
Information	CFG	This notification is generated while trying to load/save the configuration, indicating the files which are opened.	No action required.

Comments? infodev@avaya.com

Chapter 12: Config messages

Config information messages

CFG - Could not acquire FLASH sem

Type/Severity	Source	Description	Remedial Action
Information	CFG	An extreme concurrency faced when you copy or auto-synchronize the configuration.	Retry the last command.

Comments? infodev@avaya.com

Chapter 13: CFM Messages

CFM Information Messages

CFM: ERROR adding port filters for VLAN %d - no resources

Type/Severity	Source	Description	Remedial Action
Information	SPB	Error adding port filters.	No action required.

Comments? infodev@avaya.com

Chapter 14: DAI messages

DAI information messages

DAI: ARP packet with invalid IP/MAC binding dropped on untrusted port %d/%d. ARP packet has MAC source %02x-%02x-%02x-%02x-%02x-%02x.

Type/Severity	Source	Description	Remedial Action
Information	DAI	ARP packet is ingressed on a DAI untrusted port with a MAC address and IP address that does not match any entries in the binding table. This causes the packet to be dropped.	Potential intruder. Isolate the offender.

Comments? infodev@avaya.com

Chapter 15: DHCP Relay messages

DHCP Relay information messages

Error disabling global DHCP relay errCode

Type/Severity	Source	Description	Remedial Action
Information	DHCPR	The DHCP relay cannot be globally disabled as the appropriate filter could not be uninstalled (other DHCP application is using it).	Redo the QoS filter allocations, and retry to disable the DHCPR.

Error enabling global DHCP relay errCode

Type/Severity	Source	Description	Remedial Action
Information	DHCPR	The DHCP relay cannot be enabled globally as the appropriate filter cannot be installed (other DHCP application has already installed it).	Redo the QoS filter allocations, and retry to enable the DHCPR.

Comments? infodev@avaya.com

Chapter 16: DHCP Snooping messages

DHCP Snooping information messages

DHCP packet with mismatch MAC address dropped on un-trusted port unit# port# mac(MAC ADDRESS)

Type/Severity	Source	Description	Remedial Action
Information	DHCP Snoop	DHCP packet with the ethernet source MAC address not matching with the DHCP client hardware MAC address ingressed on an DHCP Snoop untrusted port. This violates the DHCP Snoop integrity check and the packet is dropped.	Isolate the offender.

DHCP Snoop DHCP ACK dropped on untrusted port unit# port# (not allowed on untrusted port)

Type/Severity	Source	Description	Remedial Action
Information	DHCP Snoop	DHCP ACK reply packet ingressed on an untrusted DHCP Snoop port. This violates the DHCP Snoop integrity check and the packet is dropped.	Isolate the offender.

DHCP Snoop DHCP binding table is full additional DHCP clients will not be added to the binding table

Type/Severity	Source	Description	Remedial Action
Information	DHCP Snoop	The maximum number of DHCP binding entries (1024) reached. Any additional DHCP client entries will not be added to the binding table.	Scale down the number of DHCP clients.

DHCP Snoop DHCP NAK dropped on untrusted port unit# port# (not allowed on untrusted port)

Type/Severity	Source	Description	Remedial Action
Information	DHCP Snoop	DHCP NAK reply packet ingressed on an DHCP Snoop untrusted port. This violates the DHCP Snoop integrity check and the packet is dropped.	Isolate the offender.

DHCP Snoop DHCP OFFER dropped on untrusted port unit# port# (not allowed on untrusted port)

Type/Severity	Source	Description	Remedial Action
Information	DHCP Snoop	DHCP OFFER reply packet ingressed on an DHCP Snoop untrusted port. This violates the DHCP Snoop integrity check and the packet is dropped.	Isolate the offender.

Comments? infodev@avaya.com

DHCP Snoop: DHCP packet dropped on port %d/%d - static entry with the same MAC %02x-%02x-%02x-%02x-%02x-%02x in binding table

Type/Severity	Source	Description	Remedial Action
Information	DHCP Snoop	DHCP packet ingressed on thespecified port is dropped as a static entry with the same MAC address as the DHCP client MAC address is found in the binding table. This violates the DHCP Snoop integrity check and the packet is dropped.	No action required.

DHCP Snoop DHCP RELEASE DECLINE dropped on untrusted port unit# port# because MAC Addr(MACaddress) is associated to port unit# port#

Type/Severity	Source	Description	Remedial Action
Information	DHCP Snoop	DHCP RELEASE or DECLINE packet with the DHCP client hardware MAC address and client port from the binding table ingressed on a different DHCP Snoop untrusted port. This violates the DHCP Snoop integrity check and the packet is dropped.	Isolate the offender.

DHCP Snoop DHCP RELEASE DECLINE dropped on untrusted port unit# port# (MAC Addr(MACaddress) does not exist in binding table)

Type/Severity	Source	Description	Remedial Action
Information	DHCP Snoop	DHCP RELEASE or DECLINE packet with the DHCP client hardware MAC address is not found in the binding table ingressed on a DHCP Snoop untrusted port. This violates the DHCP Snoop integrity check and the packet is dropped.	Isolate the offender.

DHCP Snoop DHCP REQUEST dropped on un-trusted port unit# port# due to source MAC address(MAC ADDRESS) not matching DHCP client

Type/Severity	Source	Description	Remedial Action
Information	DHCP Snoop	DHCP packet with the ethernet source MAC address not matching with the DHCP client hardware MAC address ingressed on an DHCP Snoop untrusted port. This violates the DHCP Snoop integrity check and the packet is dropped.	Isolate the offender.

Comments? infodev@avaya.com

DHCP Snoop NTP is not synchronized; external save restore of DHCP snooping entries not possible

Type/Severity	Source	Description	Remedial Action
Information	DHCP SNOOP	The external actions (Restore or Save) not possible, as the Unit (S)NTP server is not synchronized.	Make sure time source is properly set to (S)NTP and the server is synchronized.

DHCP Snoop DHCP snooping entry entry number not restored due to MAC conflict

Type/Severity	Source	Description	Remedial Action
Information	DHCP SNOOP	Binding entry could not be restored due to MAC conflict.	No action required.

DHCP Snoop DHCP snooping entry entry number not restored due to parsing failure

Type/Severity	Source	Description	Remedial Action
Information	DHCP SNOOP	Binding entry could not be restored due to various parsing failures.	Check and modify the external-save file for unexpected modifications in entry syntax.

DHCP Snoop DHCP snooping binding table saved successfully to USB unit unit#

Type/ Severity	Source	Description	Remedial Action
Information	DHCP SNOOP	External-save/restore occurred successfully on the mentioned target.	No action required.

DHCP Snoop DHCP snooping entry with MAC MacAddress not restored on invalid interface unit# port#

Type/Severity	Source	Description	Remedial Action
Information	DHCP SNOOP	Binding entry could not be restored due to an invalid interface (unit/ port combination read from external file is no longer available or invalid altogether).	Check the unit/port combinations in the external-save file with your actual topology, and modify the external-save file if necessary.

DHCP Snoop DHCP snooping binding table saved successfully to TFTP address

Type/Severity	Source	Description	Remedial Action
Information	DHCP SNOOP	External-save/restore occurred successfully on the mentioned target.	No action required.

Comments? infodev@avaya.com

DHCP Snoop DHCP snooping binding table save to USB unit unit# failed

Type/Severity	Source	Description	Remedial Action
Information	DHCP SNOOP	External-save/restore occurred successfully on the mentioned target.	No action required.

DHCP Snoop DHCP snooping binding table save to TFTP address A.B.C.D IPv6_address failed

Type/Severity	Source	Description	Remedial Action
Information	DHCP SNOOP	External-save/restore was unsuccessful on the mentioned target.	No action required.

DHCP Snoop DHCP snooping binding table restored successfully from USB unit unit#

Type/Severity	Source	Description	Remedial Action
Information	DHCP SNOOP	External-save/restore was unsuccessful on the mentioned target.	Check TFTP connection or the USB target for availability.

DHCP Snoop DHCP snooping binding table restore from TFTP address A.B.C.D IPv6_address failed

Type/Severity	Source	Description	Remedial Action
Information	DHCP SNOOP	External-save/restore was unsuccessful on the mentioned target.	Check TFTP connection or the USB target for availability.

DHCP Snoop: DHCP snooping entry 0x%08x not restored on trusted interface %d/%d

Type/Severity	Source	Description	Remedial Action
Information	DHCP SNOOP	Binding entry could not be restored because the interface of the externally saved entry is currently configured as DHCPSN trusted	Check configuration.

DHCP Snoop: DHCP snooping entry with MAC %02x-%02x-%02x-%02x-%02x-%02x not restored (invalid Vlan %d)

Type/Severity	Source	Description	Remedial Action
Information	DHCP SNOOP	External-save entry could not be restored due to an invalid VLAN.	Compare external entry VLAN against currently configured VLANs and change configuration if necessary.

DHCP Snoop DHCP snooping binding table restore from USB unit unit# failed

Type/Severity	Source	Description	Remedial Action
Information	DHCP SNOOP	External-save/restore was unsuccessful.	Check TFTP connection or the USB target for availability.

Comments? infodev@avaya.com

DHCP Snoop DHCP snooping binding table restored successfully from TFTP address

Type/Severity	Source	Description	Remedial Action
Information	DHCP SNOOP	External-save/restore was unsuccessful.	Check TFTP connection or the USB target for availability.

DHCP Snoop DHCP snooping entry entry number not restored due to expired lease

Type/Severity	Source	Description	Remedial Action
Information	DHCP SNOOP	Binding entry could not be restored as the lease expired.	No action required.

DHCP snooping entry with MAC %02x-%02x-%02x-%02x-%02x-%02x not restored (invalid Vlan %d)

Type/Severity	Source	Description	Remedial Action
Information	DHCPSNOOP	The message is logged with the SNMP trap bsDhcpSnoopingExtSaveEntryInvalidVlan. /* b45.5.17.0.17 */ This notification is generated when a DHCP snooping binding entry is not restored from an external file on a invalid VLAN.	No action required.

DHCP Snoop: DHCP snooping binding table saved successfully to SFTP address

Type/Severity	Source	Description	Remedial Action
Information	DHCPSNOOP	The message is logged with the SNMP Trap: bsDhcpSnoopingExtSaveSFTPSyncSuccess. /* 1.3.6.1.4.1.45.5.17.0.18 */ This notification is generated when a DHCP snooping binding entry is successfully saved to external file with SFTP.	No action required.

DHCP Snoop: DHCP snooping binding table save to SFTP address

Type/Severity	Source	Description	Remedial Action
Information	DHCP Snooping	Error while saving the DHCP binding table to SFTP server.	Check connection and configuration.

DHCP Snoop: DHCP snooping binding table succesfully restored from SFTP address

Type/Severity	Source	Description	Remedial Action
Information	DHCPSNOOP	The message is logged with the SNMP Trap: bsDhcpSnoopingExtSaveSFTPRestoreSuccess /* 1.3.6.1.4.1.45.5.17.0.20 */ This notification is generated when a DHCP snooping binding entry is restored successfully from an external file with SFTP.	No action required.

Comments? infodev@avaya.com

DHCP Snoop: DHCP snooping binding table restore from SFTP address

Type/Severity	Source	Description	Remedial Action
Information	DHCPSNOOP	The message is logged with the SNMP Trap: bsDhcpSnoopingExtSaveSFTPRestoreFailure /* 1.3.6.1.4.1.45.5.17.0.21 */ This notification is generated when a DHCP snooping binding entry is not restored from an external file with SFTP.	No action required.

DHCP Snoop: DHCP snooping entry 0x%08x not restored on trusted interface %d/%d

Type/Severity	Source	Description	Remedial Action
Information	DHCPSNOOP	BsDhcpSnoopingExtSaveEntryIfTrustedConflict /* b45.5.17.0.22 */.	No action required.

Comments? infodev@avaya.com

Chapter 17: Download messages

Download warning messages

Error accessing Image File

Type/Severity	Source	Description	Remedial Action
Serious	Console	The system could not find the image file.	Enter a valid image file name

Error Bad Image Checksum

Type/Severity	Source	Description	Remedial Action
Serious	Console	The system indicated a Bad Image Checksum.	Enter a different image.

Error reading Image File

Type/Severity	Source	Description	Remedial Action
Serious	Console	The system could not read the image file.	Enter a valid image.

Failed to Create a Watchdog

Type/Severity	Source	Description	Remedial Action
Serious	Console	The system failed to create a watchdog.	Report the error.

Failed to Read Image from Memory

Type/Severity	Source	Description	Remedial Action
Serious	Console	The system failed to read image from memory.	Retry the process again.

Memory Allocation Error

Type/Severity	Source	Description	Remedial Action
Serious	Console	The system failed to get memory buffer.	Report the error.

Not Enough Memory

Type/ Severity	Source	Description	Remedial Action
Serious	Console	This message appears when there is not enough buffer	Report the error.

TFTP Failed

Type/Severity	Source	Description	Remedial Action
Serious	Console	The system failed to get an image through the TFTP.	Check the TFTP server.

Comments? infodev@avaya.com

Memory on unit %d is under %d MBytes.

Type/ Severity	Source	Description	Remedial Action
Critical	Memory Tool	The system memory has dropped under a certain value.	Call Avaya to collect memory information. Monitor free memory and prepare for rebooting the device if the memory continues to drop.

Comments? infodev@avaya.com

Chapter 18: EAP messages

EAP information messages

Allowed connection attempt from user :

Type/Severity	Source	Description	Remedial Action
Information	RADIUS	Radius - allowed connection attempt for user starting with the given name.	No action required.

Disallowed connection Access Reject for user

Type/Severity	Source	Description	Remedial Action
Information	RADIUS	Radius - disallowed connection attempt for user starting with given name due to invalid user credentials.	Correct the user-configuration at the radius server when needed; also make sure the username and password entered are correct.

Disallowed connection Invalid SvcType for user

Type/Severity	Source	Description	Remedial Action
Information	RADIUS	Radius - disallowed connection attempt for user starting with given name due to invalid service type.	Send correct svc-type from radius-server when needed.

EAP Failed qpa-RoleAssociation unitPort ifIndex macHi xx-xx macLo xx-xx-xx-xx

Type/Severity	Source	Description	Remedial Action
Information	EAP-Filter Manager	The EAP User Based Policy Role Association failed at the given unit port (ifIndex) for given MAC address	Show QoS agent; make sure the UBP is enabled; or enable as needed; Show QoS diag and check if filters are available.

EAP GVlan Disabled for unitPort ifIndex - GVlan(vid) in different stg(id)

Type/Severity	Source	Description	Remedial Action
Information	EAP-VLAN (QDT)	The EAP failed to apply Guest VLAN since new Guest VLAN ID is in a different spanning tree group than the current port VLAN; GVLAN disabled for that port.	Show VLAN; show interfaces; show spanning-tree commands ; reconfigure VLANs in spanning tree groups as needed, and re-enable EAP on the port.

EAP Invalid RAV ID

Type/ Severity	Source	Description	Remedial Action
Information	EAP-VLAN (QDT)	The EAP failed to apply Radius Assigned VLAN since it is not an active VLAN at the switch.	show VLAN VID; show interfaces; show spanning tree commands; And make sure the VLAN is active.

Comments? infodev@avaya.com

EAP Invalid Vlan ID vid configured for port num

Type/Severity	Source	Description	Remedial Action
Information	EAP	The EAP VLAN ID received is not active for that port.	Show VLAN VID; show interfaces; show spanning-tree commands ; make sure that the VLAN is active; then re-authenticate at the port.

EAP Mac AuthFail - unitPort <unit-portnum> macHi <xx-xx> macLo <xx-xx-xx-xx>

Type/Severity	Source	Description	Remedial Action
Information	EAP	EAP Debug only - Eng Menu - EAP removed MAC on given port for given mac address on aborting PAE state machine - Not Used	No action required.

EAP Unable to Reserve EapAdmin Filter Resources rc retCode unitPort ifIndex

Type/Severity	Source	Description	Remedial Action
Information	EAP-Filter Manager	The EAP Filter Reservation Failed (5520 and 5530) with the given filter manager return code for the given unit port (ifIndex) upon admin change from authorised to unauthorised or auto	Show QoS diag and check if filters are available; adjust the resource usage if required.

EAP Unable to Reserve Filter Resources rc retCode unitPort ifIndex Force- Unauthorised

Type/Severity	Source	Description	Remedial Action
Information	EAP-Filter Manager	The EAP Filter Reservation Failure (5520 and 5530) with given filter manager return code for given unit-port (ifIndex); port is now set to force unauthorised and is blocking.	Show QoS diag and check if filters are available; adjust the resource usage if required.

EAP Unable to UnReserve EapAdmin Filter Resources rc retCode unitPort ifIndex

Type/Severity	Source	Description	Remedial Action
Information	EAP-Filter Manager	The EAP Filter Release Failure with the given filter manager return code for given unit port (ifIndex) upon admin change to force authorised.	Show QoS diag and check if filters are available; try filter allocations again and disable or enable EAP.

EAP Unable to UnReserve Filter Resources rc retCode unitPort unit-portnum

Type/Severity	Source	Description	Remedial Action
Information	EAP-Filter Manager	The EAP is unable to release filters with given filter manager return code for given unit port (ifIndex).	Show QoS diag and check if filters are available; adjust the resource usage if required.

Comments? infodev@avaya.com

EAP Failed qpa-RoleAssociation unitPort 0x%x mac %08x%04x

Type/Severity	Source	Description	Remedial Action
Information	QoS	A UBP filter could not be installed because of a QoS speciffic error.	Check QoS resources on port.

Got UserPolicy from Radius but UBP disabled - unitPort 0x%x mac %08x%04x

Type/Severity	Source	Description	Remedial Action
Information	QoS	A UBP filter could not be installed because UBP is not enabled from EAP.	Enable UBP.

EAP CDT Error

Type/Severity	Source	Description	Remedial Action
Information	CDT	EAP will not correctly receive events about MACs from CDT.	No Action Required

EAP Error - Failed to free mac info memory

Type/Severity	Source	Description	Remedial Action
Information	EAP	A NEAP client could not be deleted from the list.	Reboot the stack.

EAP Error - Default

Type/Severity	Source	Description	Remedial Action
Information	EAP	Wrong EAP parameter.	No Action Required.

EAP Failed to add host, max number of clients reached

Type/Severity	Source	Description	Remedial Action
Information	EAP	EAP already reached the maximum number of clients limit on a port.	Increase the number of eap-mac-max clients.

EAP Could not process pkt

Type/Severity	Source	Description	Remedial Action
Information	EAP	EAP received a packet with length smaller than the header size or greater than the maximum limit.	No action required.

EAP Bad pkt id

Type/Severity	Source	Description	Remedial Action
Information	EAP	EAP received a packet with another ID than expected.	No action required.

Comments? infodev@avaya.com

EAP Bad pkt len

Type/Severity	Source	Description	Remedial Action
Information	EAP	EAP received an EAPoL packet greater than 1500 bytes.	No action required.

EAP Error while sending Access Violation Trap

Type/Severity	Source	Description	Remedial Action
Information	EAP	EAP cannot send an Access Violation Trap	No action required.

EAP NULL pkt to send on Success

Type/Severity	Source	Description	Remedial Action
Information	EAP	An error appeared when creating the message to be sent for supplicant	No action required.

EAP Error while sending RAV Error Trap

Type/Severity	Source	Description	Remedial Action
Information	EAP	EAP cannot send a Radius Assigned VLAN Error Trap.	No action required.

EAP Vlan Change Aborted

Type/Severity	Source	Description	Remedial Action
Information	STP	EAP could not add a port to a VLAN that is in a different STG than the STG where the port is.	Change the STG of the VLAN.

EAP IMC Memory allocation error

Type/Severity	Source	Description	Remedial Action
Information	IMC	EAP could not allocate memory for an Inter Module Communication message	Reboot the stack.

EAP IMC Failed to send message

Type/Severity	Source	Description	Remedial Action
Information	IMC	EAP could not send an Inter Module Communication message.	Reboot the stack.

EAP Reached Mac Intruder Count

Type/Severity	Source	Description	Remedial Action
Information	EAP	EAP reached the maximum number of intruders on a port.	Check the number of intruders per port.

Comments? infodev@avaya.com

EAP Error Radius - ifIndex not found

Type/Severity	Source	Description	Remedial Action
Information	Radius	Radius received a wrong port number for which to send a response	No action required.

Non-EAP Client blocked (Block Subsequent MAC Authentication): Different VID than expected

Type/Severity	Source	Description	Remedial Action
Information	EAP	A Non-EAP client was blocked because it had a different Radius Assigned VLAN than the previous one	Check the Attributes sent by RADIUS Server.

Non-EAP Client blocked (Block Subsequent MAC Authentication): EAP Use Rav Not enabled

Type/Severity	Source	Description	Remedial Action
Information	EAP	An EAP client was blocked because Non-EAP Radius Assigned VLAN is not enabled	Check the Attributes sent by RADIUS Server.

EAP Client blocked (Block Subsequent MAC Authentication): Invalid VID

Type/Severity	Source	Description	Remedial Action
Information	EAP	An EAP client was blocked because it had an invalid Radius Assigned VLAN.	Check the Attributes sent by RADIUS Server.

EAP Client blocked (Block Subsequent MAC Authentication): Different VID than expected

Type/Severity	Source	Description	Remedial Action
Information	EAP	An EAP client was blocked because it had a different Radius Assigned VLAN than the previous one.	Check the Attributes sent by RADIUS Server.

No Response from RADIUS Server

Type/Severity	Source	Description	Remedial Action
Information	Radius	FailOpenVLAN Continuity mode was triggered because there was no response from Radius for a MAC address of a certain client.	No action required.

EAP Failed to add host, memory allocation error

Type/Severity	Source	Description	Remedial Action
Information	EAP	EAP could not allocate memory for a new EAP client.	Reboot the stack.

EAP Neap port was not member of any vlan

Type/Severity	Source	Description	Remedial Action
Information	EAP	A Non-EAP port was added to either GuestVLAN or VLAN 1, because it was not a member of any VLAN.	No action required.

Comments? infodev@avaya.com

EAP warning messages

EAP Task spawn error

Type/Severity	Source	Description	Remedial Action
Serious	EAP	The EAP application task could not be started.	Reboot the stack.

EAP Failed to create dyna global arrays

Type/Severity	Source	Description	Remedial Action
Serious	EAP	EAP could not initialize some of the data regarding global or port-specific info detailed in the “Could not create global arrays” log.	Reboot the stack.

EAP Message queue error

Type/Severity	Source	Description	Remedial Action
Serious	EAP	EAP could not initialize the EAP message queue.	Reboot the stack.

EAP Error: Reached maximum number of messages in the queue

Type/Severity	Source	Description	Remedial Action
Serious	EAP	EAP received too many messages from other applications.	Reboot the stack.

EAP NVRAM read system admin state error

Type/Severity	Source	Description	Remedial Action
Serious	EAP	EAP could not read the global EAP setting from NVRAM	Reboot the stack.

EAP NVRAM read port admin state error

Type/Severity	Source	Description	Remedial Action
Serious	EAP	EAP could not read the port EAP admin setting from NVRAM	Reboot the stack.

EAP NVRAM read system ubp state error

Type/Severity	Source	Description	Remedial Action
Serious	EAP	EAP could not read the global UBP setting from NVRAM	Reboot the stack.

EAP NVRAM open error

Type/Severity	Source	Description	Remedial Action
Serious	EAP	EAP could not open the NVRAM file to write settings.	Reboot the stack.

Comments? infodev@avaya.com

EAP NVRAM write error

Type/Severity	Source	Description	Remedial Action
Serious	EAP	EAP could not write settings in the NVRAM file.	Reboot the stack.

EAP Failed initialize global arrays

Type/Severity	Source	Description	Remedial Action
Serious	EAP	EAP could not initialize data about global or ports admin state	Reboot the stack.

NEAP Accounting - Memory allocation failure

Type/Severity	Source	Description	Remedial Action
Serious	EAP	A NEAP accounting packet could not be allocated.	Reboot the stack.

EAP Memory allocation error

Type/Severity	Source	Description	Remedial Action
Serious	EAP	EAP could not allocate memory to receive or send a packet.	Reboot the stack.

Comments? infodev@avaya.com

Chapter 19: Exception messages

Exception critical messages

Sw Exception

Type/ Severity	Source	Description	Remedial Action
Critical	Exception	A task caused an exception and is suspended. The exception information is logged and can be accessed through the CLI.	The Exception information contains the problem task, the exception type, the register values, the exception stack trace and memory of the related DRAM area. With this information, you can find out the cause of the exception. (The most common method is to follow the stack trace).

Comments? infodev@avaya.com

Chapter 20: Flash Driver messages

Flash Driver critical messages

Download - DL_CKSUM_ACK_ERROR

Type/Severity	Source	Description	Remedial Action
Critical	Flash Driver	This message appears when the image on NBU fails checksum validation.	Retry or download another image.

Download - DL_PROGRAM_STATUS_ACK_ERROR

Type/Severity	Source	Description	Remedial Action
Critical	Flash Driver	This message appears when all NBUs succeed in programming the image.	Retry or reboot the switch

Download - DL_START_PROGRAM_FLASH_ACK_ERROR

Type/Severity	Source	Description	Remedial Action
Critical	Flash Driver	This message appears when not all NBUs succeed in programming image.	Retry or reboot the switch.

Download - Error Failed to get the dl resource.

Type/Severity	Source	Description	Remedial Action
Critical	Flash Driver	The system failed to access flash for the image download.	Retry or reboot the switch

Download - Error Watchdog expire No Ack from NBUs download MSG # message ID

Type/Severity	Source	Description	Remedial Action
Critical	Flash Driver	Tthe watchdog timer expired waiting for acknowledgements from the NBUs during the image programming.	Retry or reboot the switch

Download - Failed to get buffer

Type/Severity	Source	Description	Remedial Action
Critical	Flash Driver	The system failed to obtain the data buffer for downloading the image.	Retry or reboot the switch

Download - Failed to malloc for buffer

Type/Severity	Source	Description	Remedial Action
Critical	Flash Driver	The system does not have enough memory to download the image in to it.	Retry or reboot the switch.

Comments? infodev@avaya.com

Download - Failed to start a watchdog

Type/Severity	Source	Description	Remedial Action
Critical	Flash Driver	The system failed to start the watchdog timer for image programming process.	Retry or reboot the switch

Download - Image Checksum Error

Type/Severity	Source	Description	Remedial Action
Critical	Flash Driver	This message appears when the Checksum in the image is not the same as the computed one.	Retry or download another image.

Download - Largest mem blk DL_SYSMEM_RESERVED

Type/Severity	Source	Description	Remedial Action
Critical	Flash Driver	The system does not have enough memory to download the image into it.	Retry or reboot the switch.

Download - NBU Block Checksum Error

Type/Severity	Source	Description	Remedial Action
Critical	Flash Driver	The image on NBU failed the Checksum validation.	Retry or download another image.

Download - NBU DL_PROGRAM_STATUS ERROR

Type/Severity	Source	Description	Remedial Action
Critical	Flash Driver	This message appears when not all NBUs succeed in programming the image.	Retry, download another image, or reboot the stack.

Download - TFTP timeout OR image file not found

Type/Severity	Source	Description	Remedial Action
Critical	Download Task	The system detected an error: TFTP timeout	Retry or reboot the switch

Download - tftpXfer failed

Type/Severity	Source	Description	Remedial Action
Critical	Flash Driver	The system detected an error in fetching the download resource.	Retry or reboot the switch.

FSH - Error Calling taskLock() returns Error

Type/Severity	Source	Description	Remedial Action
Critical	Flash Driver	This message appears when the task is unable to disable the context switching for the flash access.	Retry or reboot the switch.

Comments? infodev@avaya.com

FSH - Error Failed to erase flash sector

Type/Severity	Source	Description	Remedial Action
Critical	Flash Driver	The system is unable to erase the flash sector to program the agent image.	Retry or reboot the switch.

FSH - Error Failed to lock flash sector

Type/Severity	Source	Description	Remedial Action
Critical	Flash Driver	The system is unable to lock the flash sector in order to prevent programming or erasing.	Retry or reboot the switch.

FSH - Error Failed to program flash

Type/Severity	Source	Description	Remedial Action
Critical	Flash Driver	The system is unable to write the image on flash.	Retry or reboot the switch.

FSH - Error Failed to unlock flash sector

Type/Severity	Source	Description	Remedial Action
Critical	Flash Driver	The system failed to unlock the flash sector in order to allow programming or erasing.	Retry or reboot the switch.

FSH - Error Failed to write to flash address

Type/Severity	Source	Description	Remedial Action
Critical	Flash Driver	The system could not program the flash memory.	Reboot the switch.

FSH - Time to Download the Image number seconds

Type/Severity	Source	Description	Remedial Action
Critical	Download Task	This message indicates the time needed to download the image.	No action required.

FSH - Time to Program the Image to flash number seconds

Type/Severity	Source	Description	Remedial Action
Critical	Download Task	This message indicates the time needed to program the image.	No action required.

Reset - Error Failed to get the Reset sem

Type/Severity	Source	Description	Remedial Action
Critical	Flash Driver	The system failed to get ownership of the reset semaphore to prevent reset during download.	Retry the operation.

Comments? infodev@avaya.com

Flash Driver warning messages

Download - image type image image version programmed successfully

Type/Severity	Source	Description	Remedial Action
Serious	Download Task	This is an informational message.	No action required.

Flash Driver information messages

DosFs - Error File not closed

Type/Severity	Source	Description	Remedial Action
Information		The system detected an error in closing the file.	Retry the operation.

Comments? infodev@avaya.com

Chapter 21: GBIC Messages

GBIC Information Messages

Notice: DAC Cable on %s is below HW rev "H" and may cause link issues with a small number of PHYs

Type/Severity	Source	Description	Remedial Action
Information	PDT	Informs the user that he has inserted an outdated HW revision DAC.	Replace with DAC that has HW Revision “H” or above.

Warning:non-supported transceiver on %s has been detected.

Type/Severity	Source	Description	Remedial Action
Information	PDT	Informs the user that the transceiver is unsupported on a certain port.	Replace with supported transceiver.

Info: Transceiver inserted on %s

Type/Severity	Source	Description	Remedial Action
Information	PDT	The transceiver has been inserted on a certain unit/ port, having a specific vendor and type.	No action required.

Info: Transceiver removed from %s

Type/Severity	Source	Description	Remedial Action
Information	PDT	The transceiver has been removed from a certain unit/port.	No action required.

SFP internal supply voltage is at high warning level on %s

Type/Severity	Source	Description	Remedial Action
Information	Port driver	The internal supply voltage of a transceiver inserted on a certain unit/port is at high warning level.	Check pluggable part and replace if necessary.

SFP internal supply voltage is at low warning level on %s

Type/Severity	Source	Description	Remedial Action
Information	Port driver	The internal supply voltage of a transceiver inserted on a certain unit/port is at low warning level.	Check pluggable part and replace if necessary.

SFP internal supply voltage is at high alarm level on s

Type/Severity	Source	Description	Remedial Action
Information	Port driver	The internal supply voltage of a transceiver inserted on a certain unit/port	Check pluggable part and replace if necessary.

Comments? infodev@avaya.com

Type/Severity	Source	Description	Remedial Action
		is at high alarm level.	

SFP internal supply voltage is at low alarm level on %s

Type/Severity	Source	Description	Remedial Action
Information	Port driver	The internal supply voltage of a transceiver inserted on a certain unit/port is at low alarm level.	Check pluggable part and replace if necessary.

SFP internal temperature is at high alarm level on %s

Type/Severity	Source	Description	Remedial Action
Information	Port driver	The internal temperature of a transceiver inserted on a certain unit/port is at high alarm level.	Check pluggable part and replace if necessary.

SFP internal temperature is at low alarm level on %s

Type/Severity	Source	Description	Remedial Action
Information	Port driver	The internal temperature of a transceiver inserted on a certain unit/port is at low alarm level.	Check pluggable part and replace if necessary.

SFP internal temperature is at high warning level on %s

Type/Severity	Source	Description	Remedial Action
Information	Port driver	The internal temperature of a transceiver inserted on a certain unit/port is at high warning level.	Check pluggable part and replace if necessary.

SFP internal temperature is at low warning level on %s

Type/Severity	Source	Description	Remedial Action
Information	Port driver	The internal temperature of a transceiver inserted on a certain unit/port is at low warning level.	Check pluggable part and replace if necessary.

SFP TX Bias current is at high warning level on %s

Type/Severity	Source	Description	Remedial Action
Information	Port driver	The TX Bias current of a transceiver inserted on a certain unit/port is at high warning level.	Check pluggable part and replace if necessary.

SFP TX Bias current is at low warning level on %s

Type/Severity	Source	Description	Remedial Action
Information	Port driver	The TX Bias current of a transceiver inserted on a certain	Check pluggable part and replace if necessary.

Comments? infodev@avaya.com

Type/Severity	Source	Description	Remedial Action
		unit/port is at low warning level.	

SFP TX Bias current is at low alarm level on %s

Type/Severity	Source	Description	Remedial Action
Information	Port driver	The TX Bias current of a transceiver inserted on a certain unit/port is at low alarm level.	Check pluggable part and replace if necessary.

SFP TX Bias current is at high alarm level on %s

Type/Severity	Source	Description	Remedial Action
Information	Port driver	The TX Bias current of a transceiver inserted on a certain unit/port is at high alarm level.	Check pluggable part and replace if necessary.

SFP TX output power is at high warning level on %s

Type/Severity	Source	Description	Remedial Action
Information	Port driver	The TX output power of a transceiver inserted on a certain unit/port is at high warning level.	Check pluggable part and replace if necessary.

SFP TX output power is at low warning level on %s

Type/Severity	Source	Description	Remedial Action
Information	Port driver	The TX output power of a transceiver inserted on a certain unit/port is at low warning level.	Check pluggable part and replace if necessary.

SFP TX output power is at high alarm level on %s

Type/Severity	Source	Description	Remedial Action
Information	Port driver	The TX output power of a transceiver inserted on a certain unit/port is at high alarm level.	Check pluggable part and replace if necessary.

SFP TX output power is at low alarm level on %s

Type/Severity	Source	Description	Remedial Action
Information	Port driver	The TX output power of a transceiver inserted on a certain unit/port is at low alarm level.	Check pluggable part and replace if necessary.

SFP Received power is at high warning level on %s

Type/Severity	Source	Description	Remedial Action
Information	Port driver	The received power of a transceiver inserted on a certain unit/port is at high warning level.	Check pluggable part and replace if necessary.

Comments? infodev@avaya.com

SFP Received power is at low warning level on %s

Type/Severity	Source	Description	Remedial Action
Information	Port driver	The received power of a transceiver inserted on a certain unit/port is at low warning level.	Check pluggable part and replace if necessary.

SFP Received power is at high alarm level on %s

Type/Severity	Source	Description	Remedial Action
Information	Port driver	The received power of a transceiver inserted on a certain unit/port is at high alarm level.	Check pluggable part and replace if necessary.

SFP Received power is at low alarm level on %s

Type/Severity	Source	Description	Remedial Action
Information	Port driver	The received power of a transceiver inserted on a certain unit/port is at low alarm level.	Check pluggable part and replace if necessary.

Comments? infodev@avaya.com

Chapter 22: Hello Module messages

Hello Module critical messages

Hello Module unable to communicate with neighbor(s) unit reset

Type/Severity	Source	Description	Remedial Action
Critical	Hello Module	This message appears under the following instances: When both stack port directions are physically up but unable to communicate with the neighboring unit(s); When one stack port direction is unable to communicate with its neighbor and the other stack port direction is not connected.The message is stored in a non-volatile memory; the presence of the message means the unit was reset.	No action required.

Hello Module error messages

Down 1 cable removed or neighbor powered off

Type/Severity	Source	Description	Remedial Action
Serious	HMOD	Link down: cable removed or neighbor powered off.	Do not remove cable, power off neighbor.

Down 2 cable removed or neighbor powered off

Type/Severity	Source	Description	Remedial Action
Serious	HMOD	Link down: cable removed or neighbor powered off.	Do not remove cable, power off neighbor.

Stack cable Down 1 is misconfigured

Type/Severity	Source	Description	Remedial Action
Error	Hello Module	This message appears when the first downstream port is mis-configured.	Connect the first downstream port to the first upstream port of the neighbor.

Stack cable Down 2 is misconfigured

Type/Severity	Source	Description	Remedial Action
Error	Hello Module	This message appears when the second downstream port is mis-configured.	Connect the second downstream port to the second upstream port of the neighbor.

Comments? infodev@avaya.com

Up 1 cable removed or neighbor powered off

Type/Severity	Source	Description	Remedial Action
Serious	HMOD	Link down: cable removed or neighbor powered off.	Do not remove cable, power off neighbor.

Up 2 cable removed or neighbor powered off

Type/Severity	Source	Description	Remedial Action
Serious	HMOD	Link down: cable removed or neighbor powered off.	Do not remove cable, power off neighbor.

Stack cable Up 1 is misconfigured

Type/Severity	Source	Description	Remedial Action
Error	Hello Module	This message appears when the first upstream port is mis-configured.	Connect the first upstream port to the first downstream port of the neighbor.

Stack cable Up 2 is misconfigured

Type/Severity	Source	Description	Remedial Action
Error	Hello Module	This message appears when the second upstream port is mis-configured.	Connect the second upstream port to the second downstream port of the neighbor.

Hello Module information messages

Down 1 cable inserted or neighbor powered on

Type/Severity	Source	Description	Remedial Action
Information	HMOD	Cable inserted, link up.	No action required.

Down 2 cable inserted or neighbor powered on

Type/Severity	Source	Description	Remedial Action
Information	HMOD	Cable inserted, link up.	No action required.

Downstream stack direction is down cable removed or neighbor powered off

Type/ Severity	Source	Description	Remedial Action
Information	Hello Module	The Downstream stack direction is down, cable removed or neighbor powered off.	Connect the downstream port to the upstream port of the neighbor. Also check if the neighbor is powered on.

Downstream stack direction is mis-configured

Type/Severity	Source	Description	Remedial Action
Information	Hello Module	This message appears when a downstream port is mis-configured.	Connect the downstream port to the upstream port of the neighbor.

Comments? infodev@avaya.com

Downstream stack direction is up cable inserted or neighbor powered on

Type/Severity	Source	Description	Remedial Action
Information	Hello Module	The Downstream stack direction is up, cable inserted and neighbor powered on. Physical link is up now.	No action required.

Up 1 cable inserted or neighbor powered on

Type/Severity	Source	Description	Remedial Action
Information	HMOD	Cable inserted, link up.	No action required.

Up 2 cable inserted or neighbor powered on

Type/Severity	Source	Description	Remedial Action
Information	HMOD	Cable inserted, link up.	No action required.

Upstream stack direction is down cable removed or neighbor powered off

Type/Severity	Source	Description	Remedial Action
Information	Hello Module	The upstream stack direction is down, cable removed or neighbor powered off.	Connect the upstream port to the downstream port of the neighbor. Also check if the neighbor is powered on.

Upstream stack direction is mis-configured

Type/Severity	Source	Description	Remedial Action
Information	Hello Module	This message appears when an upstream port is mis-configured.	Connect the upstream port to the downstream port of the neighbor.

Stack cable "Down 1" is misconfigured

Type/Severity	Source	Description	Remedial Action
Information	HMOD	Top cable of Downstream direction is misconfigured.	No action required.

Stack cable "Down 2" is misconfigured

Type/Severity	Source	Description	Remedial Action
Information	HMOD	Bottom cable of Downstream direction is misconfigured.	No action required.

Stack cable "Up 1" is misconfigured

Type/Severity	Source	Description	Remedial Action
Information	HMOD	Top cable of Upstream direction is misconfigured.	No action required.

Comments? infodev@avaya.com

Stack cable "Up 2" is misconfigured

Type/Severity	Source	Description	Remedial Action
Information	HMOD	Bottom cable of Upstream direction is misconfigured.	No action required.

Comments? infodev@avaya.com

Chapter 23: IGMP messages

IGMP critical messages

IGMP Initialization failed Error code errCode

Type/Severity	Source	Description	Remedial Action
Critical	IGMP	The IGMP initialization failed due to unavailable system resources.	Restart the system.

IGMP warning messages

IGMP Error sending database from unit unit#

Type/Severity	Source	Description	Remedial Action
Serious	IGMP	The IGMP database cannot be sent to a unit in the stack.	No action required.

IGMP Error sending group database from unit unit#

Type/Severity	Source	Description	Remedial Action
Serious	IGMP	The IGMP Group database cannot be transmitted from	No action required.

Type/Severity	Source	Description	Remedial Action
		one unit to the other in the stack.	

IGMP information messages

IGMP Added reserved multicast address

Type/Severity	Source	Description	Remedial Action
Information	IGMP	This message appears when the unknown multicast allowed address is successfully registered on the switch.	No action required.

IGMP Exceeded reserved multicast address range #Addr numResAddrEntries+1 * #VLANs numActiveVLANs maxReservedRange

Type/Severity	Source	Description	Remedial Action
Information	IGMP	The maximum number of registered unknown allowed multicast addresses are reached.	No action required.

IGMP Maximum number of igmp enabled interfaces reached

Type/ Severity	Source	Description	Remedial Action
Serious	ipmc (igmp)	The IGMP-enabled interfaces reached the maximum limit of 256.	Disable the IGMP on interfaces that no longer need to be IGMP-enabled.

Comments? infodev@avaya.com

IGMP No hardware resource available

Type/Severity	Source	Description	Remedial Action
Information	ipmc (igmp)	The IGMP Hardware Resource Allocation Failed.	Redo the QoS filter allocations.

IGMP Proxy disabled on VLAN vlan#

Type/Severity	Source	Description	Remedial Action
Information	IGMP	Tthe IGMP proxy is disabled for a VLAN.	No action required.

IGMP Proxy enabled on VLAN vlan#

Type/Severity	Source	Description	Remedial Action
Information	IGMP	The IGMP proxy is enabled for a VLAN.	No action required.

IGMP Query Time set to num on VLAN vlan#

Type/Severity	Source	Description	Remedial Action
Information	IGMP	The “Query Time” parameter is modified for a VLAN.	No action required.

IGMP Removed reserved multicast address

Type/Severity	Source	Description	Remedial Action
Information	IGMP	The unknown allowed multicast address is unregistered on the switch.	No action required.

IGMP Robust Value set to num on VLAN vlan#

Type/Severity	Source	Description	Remedial Action
Information	IGMP	The “Robust Value” parameter is modified for a VLAN.	No action required.

IGMP Snooping disabled on VLAN vlan#

Type/Severity	Source	Description	Remedial Action
Information	IGMP	The IGMP snooping is disabled for a VLAN.	No action required.

IGMP Snooping enabled on VLAN vlan#

Type/Severity	Source	Description	Remedial Action
Information	IGMP	The IGMP snooping is enabled for a VLAN.	No action required.

IGMP SSM Range changed

Type/Severity	Source	Description	Remedial Action
Information	IGMP	The group range for IP IGMP SSM has changed.	No action required.

Comments? infodev@avaya.com

IGMP Unable to add reserved multicast address

Type/ Severity	Source	Description	Remedial Action
Information	IGMP	This message appears when an unknown multicast address registration fails.	No action required.

IGMP Unknown Multicast Filter disabled

Type/Severity	Source	Description	Remedial Action
Information	IGMP	The “Unknown Multicast No Flood” feature is disabled from the user interface.	No action required.

IGMP Unknown Multicast Filter enabled

Type/ Severity	Source	Description	Remedial Action
Information	IGMP	This message appears when the “Unknown Multicast No Flood” feature is enabled from the user interface.	No action required.

IGMP V1 router ports mask

Type/Severity	Source	Description	Remedial Action
Information	IGMP	This message appears when the list of IGMP version 1 router ports are modified.	No action required.

IGMP V2 router ports mask

Type/Severity	Source	Description	Remedial Action
Information	IGMP	This message appears when the list of IGMP version 2 router ports are modified.	No action required.

IGMP: V2 report drop on reserved GA

Type/Severity	Source	Description	Remedial Action
Information	MCMGR/ IGMP	IGMP V2 report for reserved group IP was dropped.	No action required.

IGMP: V3 report group skip on invalid GA

Type/Severity	Source	Description	Remedial Action
Information	MCMGR/ IGMP	A group record in an IGMP V3 report was skipped, as the group address is not multicast.	No action required.

IGMP: V3 report group skip on reserved GA

Type/Severity	Source	Description	Remedial Action
Information	MCMGR/ IGMP	A group record in an IGMP V3 report was skipped, as the group address is reserved.	No action required.

Comments? infodev@avaya.com

Chapter 24: IMC messages

IMC critical messages

IMC buffers of size buffer size have been exhausted buffer pool size pool size

Type/Severity	Source	Description	Remedial Action
Critical	IMC	This message appears when memory buffers used for communication between units in a stack are exhausted. The <buffer size> > varies and is measured in bytes.The <pool size> can vary for different buffer sizes and different models (ERS 25XX / 45XX / 55XX / 56XX).	Restart the system.

IMC warning messages

IMC memory allocation error packetLength = %d file %s line %d

Type/Severity	Source	Description	Remedial Action
Warning	IMC	An error occurred on IMC packet allocation.	No action required.

IMC imc_idtPacketDispatch() incorrect rcvMsgType = %s(%d)

Type/Severity	Source	Description	Remedial Action
Warning	IMC	An incorrect message type was received.	No action required.

Comments? infodev@avaya.com

Chapter 25: IP messages

IP information messages

IPT BootP Disabled (response not received from server)

Type/Severity	Source	Description	Remedial Action
Information	IPT	This message appears when the BootP mode is disabled after the stack is reset and for 10 minutes no BootP/DHCP messages are received (DUT stops sending BootP Requests).	No action required.

IPT IP Address changed by BOOTP Server

Type/Severity	Source	Description	Remedial Action
Information	IPT	The switch or the stack has received the IP address from the BOOTP Server.	No action required.

IPT: IP Address not in use (duplicate detected)

Type/Severity	Source	Description	Remedial Action
Information	Inband IP address	The IP address configured on the management VLAN was also found	Use different IP addresses.

Type/Severity	Source	Description	Remedial Action
		configured on another unit in the network.	

Gateway IP changed

Type/Severity	Source	Description	Remedial Action
Information	IPT	This message indicates that the Gateway IP has changed.	No action required.

Stack IP changed

Type/Severity	Source	Description	Remedial Action
Information	IPT	This message indicates that the Stack IP has changed.	No action required.

Switch IP changed

Type/Severity	Source	Description	Remedial Action
Information	IPT	This message indicates that the Switch IP has changed.	No action required.

Comments? infodev@avaya.com

Chapter 26: IPFIX messages

IPFIX information messages

IPFIX enable failure

Type/Severity	Source	Description	Remedial Action
Information	IPFIX	This message indicates that the task cannot start.	No action required.

Comments? infodev@avaya.com

Chapter 27: IPMC messages

IPMC warning messages

IGMP Maximum number of igmp enabled interfaces reached

Type/ Severity	Source	Description	Remedial Action
Serious	ipmc (igmp)	The IGMP-enabled interfaces reached the maximum limit of 256.	Disable the IGMP on interfaces that no longer need to be IGMP-enabled.

IPMC information messages

IGMP No hardware resource available

Type/Severity	Source	Description	Remedial Action
Information	ipmc (igmp)	The IGMP Hardware Resource Allocation Failed.	Redo the QoS filter allocations.

IGMP SSM Range changed

Type/Severity	Source	Description	Remedial Action
Information	ipmc (igmp)	The IGMP global allowable SSM range is changed.	No action required.

Comments? infodev@avaya.com

Chapter 28: IPSG messages

IPSG information messages

Cannot disable IP Source Guard on Unit unit# Port port#

Type/ Severity	Source	Description	Remedial Action
Information	ipsg	The IPSG cannot be disabled on the specified unit/port.	Disable the MLT (if it enabled) and try again. If it fails, then reboot the switch.

IP Source Guard disabled on Unit unit# Port port#

Type/Severity	Source	Description	Remedial Action
Information	ipsg	The IP Source Guard has been disabled on the specified Unit Port.	No action required.

IP Source Guard enabled on Unit unit# Port port#

Type/Severity	Source	Description	Remedial Action
Information	ipsg	The IP Source Guard has been enabled on the specified Unit Port.	No action required.

IPSG Insufficient resources available to enable IPSG on port unit# port#

Type/Severity	Source	Description	Remedial Action
Information	ipsg	There are no enough resources available to enable the IPSG on the specified port.	Verify Qos masks and filter usage using the command: **`Show qos diag`**. Disable / delete any QoS policy or application which is no longer needed on that port.

IPSG nvRam file error param1 param2 param3

Type/Severity	Source	Description	Remedial Action
Information	ipsg	The system detected an error while trying to access the IPSG NVRAM file param1=0 (open error), param1=1 (write error), param1=2 (read error).	Retry again and if it fails, then reboot the switch.

IPSG Reached Max. IP entries supported on this port port#

Type/Severity	Source	Description	Remedial Action
Information	ipsg	The port reached the maximum number of IP entries.	Scale down the number of IPSG clients.

IPSG Reached Max. IP entries supported on this port unit# port#

Type/Severity	Source	Description	Remedial Action
Information	ipsg	The unit/port reached the maximum number of IP entries.	Scale down the number of IPSG clients.

Comments? infodev@avaya.com

IPSG Resource allocated for Ports unit# port#

Type/Severity	Source	Description	Remedial Action
Information	ipsg	The resources necessary for the specified ports cannot be allocated by the QoS application.	Retry and if it fails, then reboot the switch.

Comments? infodev@avaya.com

Chapter 29: IPv6 messages

IPv6 information messages

Duplicate address deletion failed ipv6_address

Type/Severity	Source	Description	Remedial Action
Information	IPV6	The Duplicate Address Detection procedure found a duplicate for the IPv6_address on the link.	Change the link-local ID for the IPV6 interface if the ipv6_address is in link-local scope. Remove and assign a different ipv6_address if the ipv6_address is in global scope.

Duplicate address detection succeeded ipv6_address

Type/ Severity	Source	Description	Remedial Action
Information	IPV6	The Duplicate Address Detection procedure is successfully completed for the ipv6_address, and no duplicate is found on the link.	No action required.

IPv6 enabled with hardware support and FMGR filters

Type/Severity	Source	Description	Remedial Action
Information	IPv6	IPv6 enabled with hardware support and FMGR filters.	No action required.

IPv6 enabled with hardware support only

Type/Severity	Source	Description	Remedial Action
Information	IPv6	IPv6 enabled with hardware support only.	No action required.

IPv6 malloc failure

Type/Severity	Source	Description	Remedial Action
Information	IPv6	IPv6 malloc failure.	No action required.

IPv6 Forwarding disabled due to inadequate license

Type/Severity	Source	Description	Remedial Action
Information	IPV6	The IPV6 Forwarding mode is automatically disabled as there is no valid license.	Install a valid license and enable the IPV6 forwarding.

Comments? infodev@avaya.com

Chapter 30: L3 Manager messages

L3 Manager information messages

Assertion Failure in bcm_l3_hit_check- l3sw ip=%#x,l3hw ip=%#x

Parameters	Type/Severity	Source	Description	Remedial Action
Software IP address + Hardware IP address.	Serious	IPv4 Routing	Inconsistency between software and hardware IP values at some index.	Do not connect a host for which you have a host route configured directly to the switch.

ECMP features disabled due to inadequate license

Type/Severity	Source	Description	Remedial Action
Information	L3Mgr	This message appears if the ECMP is enabled and the license is not available.	Acquire License for ECMP to enable this feature.

Failed ARP add ip addr 0xFFFFFFFF to HW hw error code

Type/Severity	Source	Description	Remedial Action
Information	L3Mgr	The configuration of L3 ARP(1) into hardware failed.	Try deleting the ARP from the software and check if the hardware configuration is successful after re-learning the ARP.

Failed MVLAN(vid) L3 ip addr ip mask

Type/Severity	Source	Description	Remedial Action
Information	L3Mgr	The system failed to configure or restore the primary or secondary management VLAN from the NVRAM. It indicates parameter (IP address or Mask) with an incorrect or conflicting value if appeared during provisioning the message on screen.	Re-configure with correct values if the message appears during provisioning the message on the screen. Re-configure the management VLAN IP/Mask if the message appears during ERS device startup.

Failed to create IP intf vid ip addr in HW hw error code

Type/Severity	Source	Description	Remedial Action
Information	L3Mgr	The interface and the L3 interface(0) configuration failed.	Check by toggling routing on the VLAN to which the interface belongs, if it still fails then use global routing toggling.

Failed route add *<ip addr/ip mask>* to HW *<hw error code>*

Type/Severity	Source	Description	Remedial Action
Warning	L3Mgr	The configuration of L3 interface(0) into hardware failed.	No action required.

Comments? infodev@avaya.com

IP blocking now 1 2 (1=ON 2=OFF)

Type/Severity	Source	Description	Remedial Action
Information	L3Mgr	The IP status is blocked on the unit when it leaves a stack.	No action required.

Maximum number of dynamic routes reached

Type/Severity	Source	Description	Remedial Action
Information	L3Mgr	The maximum number of total routes (static or dynamic) supported on the platform are reached.	Reconfigure the network so that the routes on the ERS device remain within the maximum allowed.

Comments? infodev@avaya.com

Chapter 31: LACP messages

LACP information messages

LAC MLT error on far end. 0 - 0 - 0

Type/Severity	Source	Description	Remedial Action
Information	LAC	The LACP link is selected by the system, but not participating in trafic rx/tx.	Check LACP settings on both sides. Disable/re-enable LACP on ports.

LAC No more trunk group available for LAC. 0 - 0 - 0

Type/Severity	Source	Description	Remedial Action
Information	LAC	All trunk group IDs are already allocated.	Check if an unnecessary trunk ID is used.

LAC: MLT error, partner aggregation bit not set

Type/Severity	Source	Description	Remedial Action
Information	LACP	The LACP link is selected by the system, but not participating in the traffic rx/tx because the partner port is marked as not aggregable.	Check LACP settings on both sides. Disable/re-enable LACP on ports.

LAC: MLT error, partner expired bit set.

Type/Severity	Source	Description	Remedial Action
Information	LACP	The LACP link is selected by the system, but not participating in the traffic rx/tx because the partner port is marked as expired.	Check LACP settings on both sides. Disable/re-enable LACP on ports.

LAC: MLT error, partner synchronization bit not set.

Type/Severity	Source	Description	Remedial Action
Information	LACP	The LACP link is selected by the system, but not participating in the traffic rx/tx because the partner port is marked as not synchronized.	Check LACP settings on both sides. Disable/re-enable LACP on ports.

LAC with admin key %d failed configuration verification. Bad VLAN configuration.

Type/Severity	Source	Description	Remedial Action
Information	LACP	VLAN configuration is not consistent on all trunk members.	Check VLAN config and set the same VLAN parameters for all trunk members.

Comments? infodev@avaya.com

LAC with admin key %d failed configuration verification. Bad IGMP configuration.

Type/Severity	Source	Description	Remedial Action
Information	LACP	IGMP configuration is not consistent on all trunk members.	Check IGMP configuration and set the same IGMP parameters for all trunk members.

LAC with admin key %d failed configuration verification. Bad rate-limiting configuration.

Type/Severity	Source	Description	Remedial Action
Information	LACP	Rate-limiting configuration is not consistent on all trunk members.	Check Rate-limiting configuration and set the same Rate-limiting parameters for all trunk members.

LAC with admin key %d failed configuration verification. Bad DHCP-SNOOPING configuration.

Type/Severity	Source	Description	Remedial Action
Information	LACP	DHCP-snooping configuration is not consistent on all trunk members.	Check DHCP-snooping configuration and set the same DHCP-snooping parameters for all trunk members.

LAC with admin key %d failed configuration verification. Bad ARP INSPECTION configuration.

Type/Severity	Source	Description	Remedial Action
Information	LACP	ARP-Inspection configuration is not consistent on all trunk members.	Check ARP-Inspection config and set the same ARP-Inspection parameters for all trunk members.

LAC with admin key %d failed configuration verification. Bad MAC Security configuration.

Type/Severity	Source	Description	Remedial Action
Information	LACP	MAC Security configuration is not consistent on all trunk members.	Check MAC Security configuration and set the same MAC Security parameters for all trunk members.

LAC with admin key %d failed configuration verification. Bad qos status.

Type/Severity	Source	Description	Remedial Action
Information	LACP	QOS status is not consistent on all trunk members.	Check QOS status and set the same QOS status for all trunk members.

Comments? infodev@avaya.com

LAC with admin key %d failed configuration verification. Ports have different qos config.

Type/Severity	Source	Description	Remedial Action
Information	LACP	QOS configuration is not consistent on all trunk members.	Check QOS configuration and set the same QOS parameters for all trunk members.

LAC with admin key %d failed configuration verification.Ports have different SPBM configurations.

Type/Severity	Source	Description	Remedial Action
Information	LACP	SPBM configuration is not consistent on all trunk members.	Check SPBM configuration and set the same SPBM parameters for all trunk members.

LAC with admin key %d failed configuration verification. Error #: %d-%d

Type/Severity	Source	Description	Remedial Action
Information	LACP	An error not covered by other LAC inconsistency logs.	No action required.

Comments? infodev@avaya.com

Chapter 32: Link State Tracking Messages

Link State Tracking Information Messages

LinkStateTracking: First interface %d/d went up in link state group %d, enabling downstream ports

Type/Severity	Source	Description	Remedial Action
Information	LinkStateTracking	The first upstream interface went up, downstream ports are enabled.	No action required.

LinkStateTracking: First interface mlt %d went up in link state group %d, enabling downstream interfaces

Type/Severity	Source	Description	Remedial Action
Information	LinkStateTracking	The first upstream interface (trunk) switches state to ‘up’ from ‘down’ state. LST group transitions to ‘up’ operational state.	No action required.

LinkStateTracking: Interface %d/d went down in link state group %d

Type/Severity	Source	Description	Remedial Action
Information	LinkStateTracking	One upstream member (port) switches state to ‘down’, without affecting the LST group operational state.	No action required.

LinkStateTracking: Interface %d/d went up in link state group %d

Type/Severity	Source	Description	Remedial Action
Information	LinkStateTracking	One upstream member (port) switches sate to ‘up’, without affecting the LST group operational state.	No action required.

LinkStateTracking: Interface mlt %d went down in link state group %d

Type/Severity	Source	Description	Remedial Action
Information	LinkStateTracking	One upstream member (trunk) switches state to ‘down’, without affecting the LST group operational state.	No action required.

LinkStateTracking: Interface mlt %d went up in link state group %d

Type/Severity	Source	Description	Remedial Action
Information	LinkStateTracking	One upstream member (trunk) switches state to ‘up’, without affecting the	No action required.

Comments? infodev@avaya.com

Type/Severity	Source	Description	Remedial Action
		LST group operational state.	

LinkStateTracking: Last interface %d/d went down in link state group %d, disabling downstream interfaces

Type/Severity	Source	Description	Remedial Action
Information	LinkStateTracking	The last upstream interface (port) with an ‘up’ state switches to ‘down’ state. LST group transitions to ‘down’ operational state.	No action required.

LinkStateTracking: Last interface mlt %d went down in link state group %d, disabling downstream interfaces

Type/Severity	Source	Description	Remedial Action
Information	LinkStateTracking	The last upstream interface (trunk) with an ‘up’ state switches to ‘down’ state. LST group transitions to ‘down’ operational state.	No action required.

LinkStateTracking: Interface %s went up in link state group %d

Type/Severity	Source	Description	Remedial Action
Information	Link State Tracking	Issued when one upstream member (port) switches state to *up*, without affecting the LST group operational state.	No action required.

LinkStateTracking: Interface %s went up in link state group %d

Type/Severity	Source	Description	Remedial Action
Information	Link State Tracking	Issued when one upstream member (trunk) switches state to *up*, without affecting the LST group operational state.	No action required.

LinkStateTracking: Interface %s went down in link state group %d

Type/Severity	Source	Description	Remedial Action
Information	Link State Tracking	Issued when one upstream member (port) switches state to *down*, without affecting the LST group operational state.	No action required.

LinkStateTracking: Interface %s went down in link state group %d

Type/Severity	Source	Description	Remedial Action
Information	Link State Tracking	Issued when one upstream member (trunk) switches state to *down*, without affecting the LST group operational state.	No action required.

LinkStateTracking: First interface %s went up in link state group %d, enabling downstream interfaces

Type/Severity	Source	Description	Remedial Action
Information	LinkStateTracking	Issued when all upstream interfaces are in *down* state and one (port)	No action required.

Comments? infodev@avaya.com

Type/Severity	Source	Description	Remedial Action
		switches state to *up*. This marks a LST group transition to *up* operational state.	

LinkStateTracking: First interface %s went up in link state group %d, enabling downstream interfaces

Type/Severity	Source	Description	Remedial Action
Information	Link State Tracking	Issued when all upstream interfaces are in *down* state and one (trunk) switches state to *up*. This marks a LST group transition to *up* operational state.	No action required.

LinkStateTracking: Last interface %s went down in link state group %d, disabling downstream interfaces

Type/Severity	Source	Description	Remedial Action
Information	Link State Tracking	Issued when the last upstream interface (port) with an *up* state switches to *down*state. This marks a LST group transition to *down* operational state.	No action required.

LinkStateTracking: Last interface %s went down in link state group %d, disabling downstream interfaces

Type/Severity	Source	Description	Remedial Action
Information	Link State Tracking	Issued when the last upstream interface (trunk) with an *up* state switches to	No action required.

Type/Severity	Source	Description	Remedial Action
		*down*state. This marks a LST group transition to *down* operational state.	

Comments? infodev@avaya.com

Chapter 33: MLT messages

MLT information messages

MLT ID# failed configuration verification. Error # error num

Type/Severity	Source	Description	Remedial Action
Information	MLT	The MLT #(1-32) verification check failed.	Change the configuration and re-enable the MLT.

MLT NV File error

Type/Severity	Source	Description	Remedial Action
Information	MLT	The system failed to read or write to the NVRAM file.	Run the diagnostics to see if the NVRAM is still correct.

MLT %d failed configuration verification. Bad VLAN configuration.

Parameters	Type/ Severity	Source	Description	Remedial Action
MLT trunk number.	Information	MLT	VLAN config is not consistent on all trunk members.	Check VLAN config and set the same VLAN parameters for all trunk members.

MLT %d failed configuration verification. Bad VLACP configuration

Parameters	Type/ Severity	Source	Description	Remedial Action
MLT trunk number	Information	MLT	VLACP config is not consistent on all trunk members.	Check VLACP config and set the same VLACP parameters for all trunk members.

MLT %d failed configuration verification. Bad IGMP configuration.

Parameters	Type/Severity	Source	Description	Remedial Action
MLT trunk number	Information	MLT	IGMP config is not consistent on all trunk members.	Check IGMP config and set the same IGMP parameters for all trunk members.

MLT %d failed configuration verification. Bad rate-limiting configuration.

Parameters	Type/ Severity	Source	Description	Remedial Action
MLT trunk number	Information	MLT	Rate-limit config is not consistent on all trunk members.	Check rate-limit config and set the same rate-limit parameters for all trunk members.

Comments? infodev@avaya.com

MLT %d failed configuration verification. Bad MAC learning configuration.

Parameters	Type/ Severity	Source	Description	Remedial Action
MLT trunk number	Information	MLT	Mac-learning config is not consistent on all trunk members.	Check MAC-learning config and set the same MAC-learning parameters for all trunk members.

MLT %d failed configuration verification. Bad SPBM configuration.

Parameters	Type/ Severity	Source	Description	Remedial Action
MLT trunk number	Information	MLT	SPBM config is not consistent on all trunk members.	Check SPBM config and set the same SPBM parameters for all trunk members.

Last MLT trunk was allocated by MLT. No more free trunk groups.

Type/Severity	Source	Description	Remedial Action
Information	MLT	The last free trunk group was allocated by a static MLT.	Free a trunk group no longer in need to be able to allocate another MLT trunk group.

Last MLT trunk was allocated by LAC. No more free trunk groups.

Type/Severity	Source	Description	Remedial Action
Information	MLT	The last free trunk group was allocated by a dynamic LAC.	Free a trunk group no longer in need to be able to allocate another MLT trunk group.

MLT %d failed configuration verification. Bad ARP INSPECTION configuration.

Parameters	Type/ Severity	Source	Description	Remedial Action
MLT trunk number	Information	MLT	ARP INSPECTION config is not consistent on all trunk members.	Check ARP INSPECTION config and set the same ARP INSPECTION parameters for all trunk members.

MLT %d failed configuration verification. Bad DHCP-SNOOPING configuration.

Parameters	Type/ Severity	Source	Description	Remedial Action
MLT trunk number	Information	MLT	DHCP-SNOOPING config is not consistent on all trunk members.	Check DHCP-SNOOPING config and set the same DHCP-SNOOPING parameters for all trunk members.

Comments? infodev@avaya.com

MLT %d failed configuration verification. Bad IPSG CLASS configuration.

Parameters	Type/ Severity	Source	Description	Remedial Action
MLT trunk number	Information	MLT	IPSG config is not consistent on all trunk members.	Check IPSG CLASS config and set the same IPSG CLASS parameters for all trunk members.

Comments? infodev@avaya.com

Chapter 34: MDA messages

MDA information messages

%s card inserted (in unit %s)

Parameters	Type/ Severity	Source	Description	Remedial Action
MDA model description Module ID — stack only	Information	MDA	This message appears when an MDA card is inserted.	No action required.

%s card removed (from unit %s)

Parameters	Type/ Severity	Source	Description	Remedial Action
MDA model description Module ID — stack only	Information	MDA	This message appears when MDA card is removed.	No action required.

Warning %s card unsafely removed (from unit %s)

Parameters	Type/ Severity	Source	Description	Remedial Action
MDA model description	Information	MDA	This message appears when an MDA card is	No action required.

Parameters	Type/ Severity	Source	Description	Remedial Action
Module ID — stack only			removed without first being disabled.	

Warning failed to connect to %s card (in unit %s)

Parameters	Type/ Severity	Source	Description	Remedial Action
MDA model description Module ID — stack only	Information	MDA	This message appears when the system detects MDA card physical connection issues.	Check the MDA card physical connection.

Comments? infodev@avaya.com

Chapter 35: Multicast Manager Messages

Multicast Manager Critical Messages

MCM group node corrupted:

Type/Severity	Source	Description	Remedial Action
Critical	Multicast manager	The multicast manager group note is corrupted.	No action Required

Comments? infodev@avaya.com

Chapter 36: MultiConfig messages

MultiConfig information messages

Backup configuration block # block_number in use

Type/Severity	Source	Description	Remedial Action
Information	config	The back up configuration is in use.	No action required.

Backup configuration restored from primary configuration block # block_number

Type/Severity	Source	Description	Remedial Action
Information	config	Copy the back up primary configuration to the backup configuration.	No action required.

Backup configuration updated for next active configuration block # block_number

Type/Severity	Source	Description	Remedial Action
Information	config	The back up configuration will be used for the next active configuration.	No action required.

Backup Configuration Version is updated

Type/Severity	Source	Description	Remedial Action
Information	config	The back up configuration version is updated.	No action required.

Boot: system boot status 0x%x

Parameters	Type/Severity	Source	Description	Remedial Action
Boot status	Information	MCFG (Second INFO BLOCK)	Presents the state of all configs; ex: which config is active.	No action required.

Configuration saved to nv block # block_number

Type/Severity	Source	Description	Remedial Action
Information	config	This message appears when the configuration is saved to block n.	No action required.

Error loading backup configuration block # block_number

Type/Severity	Source	Description	Remedial Action
Information	config	The system failed to load the backup configuration.	No action required.

Comments? infodev@avaya.com

Error loading configuration block %d

Type/Severity	Source	Description	Remedial Action
Information	config	The system failed to load configuration from block n.	No action required.

Error loading primary configuration block # block_number

Type/Severity	Source	Description	Remedial Action
Information	config	The system failed to load the primary configuration.	No action required.

Error saving configuration to block # block_number

Type/Severity	Source	Description	Remedial Action
Information	config	The system failed to save the configuration to block n.	No action required.

Invalid Configuration Block Number %d

Type/Severity	Source	Description	Remedial Action
Information	config	Invalid configuration block number entered.	No action required.

Invalid Configuration Magic Number

Type/Severity	Source	Description	Remedial Action
Information	config	The number that identifies the block number is	No action required.

Type/Severity	Source	Description	Remedial Action
		incorrect and is not as expected.	

Invalid Configuration Version Number

Type/Severity	Source	Description	Remedial Action
Information	config	The block version number is not recognized.	No action required.

Loading configuration block # block_number

Type/Severity	Source	Description	Remedial Action
Information	config	This message appears when the configuration is loaded from block n.	No action required.

Primary Configuration files are corrupted. Restored to default

Type/Severity	Source	Description	Remedial Action
Information	config	The default primary configuration is restored. This message may also be generated after initializing all configuration from diags, in which case, no negative impact has occurred.	No action required.

Primary Configuration Version is updated

Type/Severity	Source	Description	Remedial Action
Information	config	The primary configuration version is updated.	No action required.

Comments? infodev@avaya.com

Restore Backup Configuration to Manufacture Default

Type/Severity	Source	Description	Remedial Action
Information	config	The manufactured default back up configuration is restored.	No action required.

Successfully loaded backup configuration files

Type/Severity	Source	Description	Remedial Action
Serious	Multi Config	Successfully loaded backup configuration files.	No action required.

Restore Primary Configuration to Manufacture Default

Type/Severity	Source	Description	Remedial Action
Information	config	The manufactured default primary configuration is restored.	No action required.

Successfully loaded configuration files from block %d

Type/Severity	Source	Description	Remedial Action
Information	Multi Config	Successfully loaded configuration files.	No action required.

System: Rear-Port Mode has been set to disable (reboot required to take effect)

Type/Severity	Source	Description	Remedial Action
Information	Rear-Port	System: Rear-Port Mode has been set to disable, reboot required to take effect.	Reboot.

System: Rear-Port Mode has been set to enable (reboot required to take effect).

Type/Severity	Source	Description	Remedial Action
Information	Rear-Port	Rear-Port Mode has been set to enable. Reboot required to take effect.	Reboot.

Toggle the Agent Primary Image

Type/Severity	Source	Description	Remedial Action
Information	config	The NVRAM block can be toggled between 1 and 2.	No action required.

Configuration block %d is now in use

Type/Severity	Source	Description	Remedial Action
Information	MCFG	Logs the configuration block currently used.	No action required.

Comments? infodev@avaya.com

Successfully loaded configuration files from block %d

Type/Severity	Source	Description	Remedial Action
Information	MCFG	Logs a successful configuration read from the flash.	No action required.

Successfully loaded backup configuration files

Type/Severity	Source	Description	Remedial Action
Serious	MCFG	Logs a successful configuration read from the backup block on the Flash.	No action required.

Flash Erase Warning Sector %d Address 0x%x Erase time %d ms

Type/Severity	Source	Description	Remedial Action
Information	MCFG	Logs a slow and successful flash sector erase.	Message indicates that the flash sector is nearing its end of life. No immediate action is required, but that sector may soon become unprogrammable.

Flash Erase Failed Sector %d Address 0x%x

Type/Severity	Source	Description	Remedial Action
Information	MCFG	Logs a failed flash sector erase.	Call Avaya.

Comments? infodev@avaya.com

Chapter 37: NUQC messages

NUQC information messages

NUQC - Disabled

Type/Severity	Source	Description	Remedial Action
Information	NUQC	The NUQC feature is disabled.	No action required.

NUQC - Enabled

Type/Severity	Source	Description	Remedial Action
Information	NUQC	The NUQC feature is enabled.	No action required.

NUQC - Execution of the cli template failed

Type/Severity	Source	Description	Remedial Action
Information	NUQC	The NUQC script execution failed.	Verify the syntax of the NUQC script.

NUQC - Execution of the cli template succeded

Type/Severity	Source	Description	Remedial Action
Information	NUQC	The NUQC script executed succesfully.	No action required.

Comments? infodev@avaya.com

Chapter 38: OSPF messages

OSPF information messages

Ospf Area Mismatch RxArea ra.rb.rc.rd IntfArea ia.ib.ic.id

Type/Severity	Source	Description	Remedial Action
Information	ospf(drpmgr)	An OSPF Area mismatch is detected between the OSPF packet Area ID and the interface Area ID.	show ip ospf interface VLAN <VID>; reconfigure OSPF Area ID at the switch or at the neighbor to match.

Ospf Auth Failed IpAddr ia.ib.ic.id

Type/Severity	Source	Description	Remedial Action
Information	ospf(drpmgr)	OSPF authentication failed at the given Interface IP Address when verifying the OSPF packet.	show ip ospf interface VLAN <VID>; reconfigure OSPF authType and related information at the switch or at the neighbor to match.

Ospf Auto Virt Link Failed area a1.a2.a3.a4 rtid r1.r2.r3.r4

Type/Severity	Source	Description	Remedial Action
Information	ospf(drpmgr)	OSPF auto creation of virtual link failed as it	Show IP OSPF virtual-link to see if any of the existing ones need to be removed;

Type/Severity	Source	Description	Remedial Action
		exceeds the maximum 4 allowed.	worst case, bounce OSPF to see if this clears it.

Ospf Cost Exceeds Limit Skip route Lsid I1.I2.I3.I4 Adv-rtr a1.a2.a3.a4

Type/Severity	Source	Description	Remedial Action
Information	ospf(drpmgr)	OSPF LSA Calculated cost exceeds limit of 0xFFFFFF.	Show IP OSPF redistribute and show route-map; check metric; correct as needed; may need actions at the neighbor.

Ospf Enable Failed as Resource Unavailable

Type/Severity	Source	Description	Remedial Action
Information	ospf(drpmgr)	The system detected an OSPF Hardware Resource Allocation Failure in the ERS5510 Mode.	Re-do QoS filter allocations and restart the switch or OSPF or global routing.

Ospf Hello: RId Same as Neighbor: rtid <r1.r2.r3.r4>, IpAddr <i1.i2.i3.i4>

Type/Severity	Source	Description	Remedial Action
Information	ospf(drpmgr)	Ospf Hello received at given Interface has the same RouterId as the switch.	Show IP OSPF at the switch and at the neighbor; ensure the router IDs are different.

Comments? infodev@avaya.com

Ospf HW Mode Change:

Type/Severity	Source	Description	Remedial Action
Information	ospf(drpmgr)	The OSPF Hardware Mode changed to the given new mode.	No action required.

Ospf Invalid packet received: Pkt type <ospfPacketType>

Type/Severity	Source	Description	Remedial Action
Information	ospf(drpmgr)	The OSPF Link State Update packet received is invalid; packet is dropped.	Either lsa is too small (<20 bytes) or too big (> (1500-64 for headers); or wrong number of lsas; retry bouncing OSPF at the neighbor or redo parts of neighbor configuration.

Ospf License Is Missing, Disable OSPF

Type/Severity	Source	Description	Remedial Action
Information	ospf(drpmgr)	OSPF License is missing; inconsistency expected if the OSPF is enabled in the NVRAM configuration.	Show license; Check for available licenses; A valid license is needed for the OSPF functionality.

Ospf Nbr State Change: rtid <ra.rb.rc.rd> ipa <ia.ib.ic.id> state <neighborState>

Type/Severity	Source	Description	Remedial Action
Information	ospf(drpmgr)	OSPF Nbr State Change: for given	No action required.

Type/Severity	Source	Description	Remedial Action
		Neighbor Router ID, Address and State.	

Ospf Netmask Mismatch in Hello IpAddr ia.ib.ic.id

Type/Severity	Source	Description	Remedial Action
Information	ospf(drpmgr)	There is an OSPF Netmask Mismatch between the netmask of IP Address in the hello packet and the netmask of the Interface IP Address.	show VLAN IP VID <VLANID> at the switch and the neighbor - reconfigure IP address/ mask as needed to match.

Ospf Option Mismatch in Hello IpAddr ia.ib.ic.id RxOption optionVal IntfOption optionVal

Type/Severity	Source	Description	Remedial Action
Information	ospf(drpmgr)	OSPF Hello option Mismatch for stub or nssa area selection in the packet vs that of the interface area.	show ip ospf interface VLAN <VID> to find areaId of interface; show ip ospf area <areaID> to check if area type ; reconfigure these as needed.

Ospf Virt Nbr State Change: rtid <r1.r2.r3.r4>, virtAreaId <v1.v2.v3.v4>, state <neighborState>

Type/Severity	Source	Description	Remedial Action
Information	ospf(drpmgr)	OSPF Virtual Neighbor of given routerID and areaID changed to a given state.	No action required.

Comments? infodev@avaya.com

OspfDbg Done Global Init

Type/Severity	Source	Description	Remedial Action
Information	OSPF	Describes the start-up sequence of OSPF initializations on reboot.	No action required.

OspfDbg Init Instance vrfId=%d nodeP=0x%0x

Type/Severity	Source	Description	Remedial Action
Information	OSPF	Describes the start-up sequence of OSPF initializations on reboot.	No action required.

OspfDbg PostInit EnableOspf vrfId=%d nodeP=0x%0x

Type/Severity	Source	Description	Remedial Action
Information	OSPF	Describes the start-up sequence of OSPF initializations on reboot.	No action required.

OspfDbg PostInit Done vrfId=%d nodeP=0x%0x

Type/Severity	Source	Description	Remedial Action
Information	OSPF	Describes the start-up sequence of OSPF initializations on reboot.	No action required.

OspfDbg Started ospfTxHelloTimerTask

Type/Severity	Source	Description	Remedial Action
Information	OSPF	Describes the start-up sequence of OSPF initializations on reboot.	No action required.

OspfDbg Done NV-Restore

Type/Severity	Source	Description	Remedial Action
Information	OSPF	Describes the start-up sequence of OSPF initializations on reboot.	No action required.

OspfDbg Done Filter Init

Type/Severity	Source	Description	Remedial Action
Information	OSPF	Describes the start-up sequence of OSPF initializations on reboot.	No action required.

OspfDbg Done ReDist Init

Type/Severity	Source	Description	Remedial Action
Information	OSPF	Describes the start-up sequence of OSPF initializations on reboot.	No action required.

Comments? infodev@avaya.com

OSPF Callback function of timer is NULL

Type/Severity	Source	Description	Remedial Action
Information	OSPF	Reports an OSPF bad timer failure (ex: bad LSA received).	No action required.

OSPF Timer Link Error

Type/Severity	Source	Description	Remedial Action
Information	OSPF	Reports an OSPF bad timer failure (ex: bad LSA received).	No action required.

OSPF Timer Unlink Error

Type/Severity	Source	Description	Remedial Action
Information	OSPF	Reports an OSPF bad timer failure (ex: bad LSA received).	No action required.

OSPF Timer List is corrupted

Type/Severity	Source	Description	Remedial Action
Information	OSPF	Reports an OSPF bad timer failure (ex: bad LSA received).	No action required.

Ospf Bad Version

Type/Severity	Source	Description	Remedial Action
Information	OSPF	Reports the OSPF version mismatch.	Verify the OSPF version.

Ospf Auth Type Mismatch in Hello

Type/Severity	Source	Description	Remedial Action
Information	OSPF	Reports the OSPF authentication mismatch on the neighboring interfaces.	Verify that OSPF authentication parameters match on the neighboring interfaces.

Ospf Hello Int Mismatch in Hello

Type/Severity	Source	Description	Remedial Action
Information	OSPF	Reports the OSPF Hello interval mismatch on the neighboring interfaces.	Verify that OSPF Hello parameters match on the neighboring interfaces.

Ospf Dead Int Mismatch in Hello

Type/Severity	Source	Description	Remedial Action
Information	OSPF	Reports the OSPF Dead interval mismatch on the neighboring interfaces.	Verify that OSPF Dead Int parameters match on the neighboring interfaces.

Comments? infodev@avaya.com

Chapter 39: OOB Management Messages

OOB Management Serious Messages

Management IP: excess traffic received on Management port%s

Type/Severity	Source	Description	Remedial Action
Serious	PDT	Excess traffic received on the management port. The port is down.	Take notice of excess traffic and restart the port.

OOB Management Information Messages

Management IP: OOB port%s

Type/Severity	Source	Description	Remedial Action
Information	PDT	Management port is down.	No action required.

Management IP: OOB port%s

Type/Severity	Source	Description	Remedial Action
Information	PDT	Management port is up.	No action required.

Comments? infodev@avaya.com

Chapter 40: PIM messages

PIM information messages

Pim E-BSR change

Type/Severity	Source	Description	Remedial Action
Information	PIM	A BSR with higher priority is detected. Logged only on BSR that changes.	Check priority of the configured BSRs.

Pim Invalid packet received

Type/Severity	Source	Description	Remedial Action
Information	PIM	PIM Control packets received are not conforming to the PIMv2 RFC 2362.	Check if sending router conforms to PIMv2 specifications, or if packets are being corrupted in the network.

Pim License Is Missing Disable PIM

Type/Severity	Source	Description	Remedial Action
Information	PIM	PIM is a licensed feature. PIM can only be configured, but cannot be activated without a license.	Contact the support personnel for an appropriate license.

Pim Mode Change

Type/Severity	Source	Description	Remedial Action
Information	PIM	Change from PIM SM mode to SSM or vice-versa.	Check and ensure that a proper mode has been selected. Will lead to change in IP Multicast traffic flows in VLANs where mode has been changed.

Pim Nbr State Change Up

Type/Severity	Source	Description	Remedial Action
Information	PIM	PIM_NBR_UP: A new neighbor is detected. It occurs when a PIM Hello message is received from an active PIM router. This can result in a change in IP multicast traffic flow if this neighbor is towards RP or BSR espcially if combined with change in unicast routing.	If the same neighbor is repeatedly appearing and disappearing, this is due to congestion in the link towards this neighbor. Check to see if unicast routing is also being affected as well as CPU utilization.

PIM Neighbor status change Down

Type/Severity	Source	Description	Remedial Action
Information	PIM	PIM_NBR_DOWN: An existing neighbor has timed out. This occurs when PIM Hello messages are not received from a neighbor within 3.5 times the query interval for an active PIM interface. This may lead to changes in the IP Multicast traffic flow.	Check if the neighbor router is functional and is sending out PIM Hellos.

Comments? infodev@avaya.com

Pim RP type state

Type/Severity	Source	Description	Remedial Action
Information	PIM	This message indicates the change from dynamic to static RP or the other way around.	If changing to static RP, ensure this is configured in the entire PIM domain. Also, BSR information will be lost and will need to be re-configured if moving to Dynamic RPs.

Pim Unicast route change

Type/Severity	Source	Description	Remedial Action
Information	PIM	Unicast route towards a source or RP has changed. This can result in changes in IP multicast traffic flow. Indicates if the route towards source or RP has been modified or deleted.	Check unicast routing / ARP tables and ensure that these are correct.

Pim Virt Nbr State Change Up

Type/Severity	Source	Description	Remedial Action
Information	PIM	PIM_NBR_UP: A virtual neighbor has been configured.	Check the multicast routes and ensure proper flows, especially if used with static unicast routes.

Pim Virt Nbr State Change Down

Type/Severity	Source	Description	Remedial Action
Information	PIM	PIM_NBR_DOWN: A configured virtual neighbor is deleted.	No action required.

Comments? infodev@avaya.com

Chapter 41: PoE messages

PoE information messages

PoE Main Power Usage Off

Type/Severity	Source	Description	Remedial Action
Information	PoE	The power usage drops below the previously set threshold.	No action required.

PoE Main Power Usage On

Type/Severity	Source	Description	Remedial Action
Information	PoE	Power consumption exceeded the configured threshold.	No action required.

PoE Module Reset

Type/Severity	Source	Description	Remedial Action
Information	PoE	The PoE controller has been reset.	No action required.

PoE Port Detection Status port# Status powerStatus

Type/Severity	Source	Description	Remedial Action
Information	PoE	The system reports the current PoE port status each time a status change occurs.	No action required.

PoE The PoE power limit for port unit port has been changed to x Watts based on IP phone discovery settings

Type/Severity	Source	Description	Remedial Action
Informatiion	PoE	The PoE power limit is changed according to the PoE IP phone settings, because of the IP phone discovery mechanism.	No action required.

PoE The PoE priority for port unit port has been changed to x based on IP phone discovery settings

Type/Severity	Source	Description	Remedial Action
Information	PoE	The PoE priority changed according to the PoE IP phone settings, because of the IP phone discovery mechanism.	No action required.

Comments? infodev@avaya.com

PoE The PoE power limit for port unit port has been restored to previous value x Watts

Type/Severity	Source	Description	Remedial Action
Information	PoE	The PoE power limit is restored to the previous value, because of the IP phone disconnection.	No action required.

PoE The PoE priority for port unit port has been restored to previous value x

Type/Severity	Source	Description	Remedial Action
Information	PoE	The PoE power priority is restored to the previous value, as the IP phone is disconnected.	No action required.

The IP phone PoE limit has been changed to x Watts due to the stack modules configuration

Type/Severity	Source	Description	Remedial Action
Information	PoE	As a global parameter, the IP phone PoE limit has dynamically changed to x Watts value in stack configuration, as being the maximum common value supported on all units from stack.	No action required.

Comments? infodev@avaya.com

Chapter 42: Port Mirroring messages

Port Mirroring information messages

PM in port mirroring the old data were modified - feature Allow Traffic in mirror port was added.

Type/Severity	Source	Description	Remedial Action
Information	PMT	The Feature Allow Traffic in mirror port was added. In the upgrade situations when current image file will be replaced by the other image file in port mirroring module some features are possible to be added.	No action required.

PM in port mirroring the old data were modified - feature Many to Many was added.

Type/Severity	Source	Description	Remedial Action
Information	PMT	The Many to Many feature was added. In upgrade situations when current image file will be replaced by the other image file in port mirroring module some features are possible to be added.	No action required.

PM in port mirroring the old data were modified - feature Many to One was added.

Type/Severity	Source	Description	Remedial Action
Information	PMT	The Many to One feature was added. In upgrade situations when the current image file will be replaced by the other image file in port mirroring module some features are possible to be added.	No action required.

PM in port mirroring the old data were modified - feature Many to One with 128bits was added.

Type/Severity	Source	Description	Remedial Action
Information	PMT	The Many to One feature with 128bits was added. In upgrade situations when the current image file will be replaced by the other image file in port mirroring module some features is possible to be added.	No action required.

PM in port mirroring the old data were modified - mode type was out of range.

Type/Severity	Source	Description	Remedial Action
Information	PMT	The mode type data saved in NVRAM is out of range for one port mirroring instance (ERS 2500, ERS 4000, ERS 55xx) or for one of the four port mirroring instances (ERS56xx).	No action required.

Comments? infodev@avaya.com

PM in port mirroring the old data were modified - monitored portA was out of range.

Type/Severity	Source	Description	Remedial Action
Information	PMT	The monitored port A data saved in the NVRAM is out of range for one port mirroring instance (ERS 2500,ERS 4000,ERS 55xx) or for one of the four port mirroring instances (ERS56xx).	No action required.

PM in port mirroring the old data were modified - monitored portB was out of range.

Type/Severity	Source	Description	Remedial Action
Information	PMT	The monitored port B data saved in the NVRAM is out of range for one port mirroring instance (ERS 2500, ERS 4000, ERS 55xx) or for one of the four port mirroring instances (ERS 56xx).	No action required.

PM in port mirroring the old data were modified - NVRAM file structure was changed.

Type/Severity	Source	Description	Remedial Action
Information	PMT	NVRAM file structure was changed. This message appears when the downgrade/upgrade of images is completed.	No action required.

PM in port mirroring the old data were modified - probe port was out of range.

Type/Severity	Source	Description	Remedial Action
Information	PMT	The probe port data saved in the NVRAM is out of range for one port mirroring instance (ERS 2500, ERS 4000, ERS 55xx) or for one of the four port mirroring instances (ERS 56xx).	No action required.

PM some port mirroring messages were stored to be displayd with delay.

Type/Severity	Source	Description	Remedial Action
Information	PMT	This message appears when the SYSLOG task runs before the port mirroring initialization function is called from the PORT MIRRORING task. This message is written first and is succeeded every time by the other port mirroring messages.	No action required.

PM unable to create mirror for instance instance number due to lack of available filter resources

Type/Severity	Source	Description	Remedial Action
Information	PM	Port mirroring initialization failed due to lack of hardware filters.	Disable other features which are using the filter resources. Use **`show qos diag`** command to find which applications are using the filter resources.

Comments? infodev@avaya.com

PM: in port mirroring the old data were modified - feature RSPAN was added

Type/Severity	Source	Description	Remedial Action
Information	Port Mirroring	After upgrade, the RSPAN feature was added	No action required.

PM: instance %d has been deleted because of insufficient HW resource

Type/Severity	Source	Description	Remedial Action
Information	Port Mirroring	The instance is erased, because no hardware resources are available for the current port mirroring configuration.	No action required.

Comments? infodev@avaya.com

Chapter 43: QoS messages

QoS critical messages

802.1p user priority mapping modifications not supported

Type/Severity	Source	Description	Remedial Action
Critical	QoS	The system detected an internal error; the specified modifier option is not supported.	Try again later, reset the QoS agent or reset the unit.

Access assignment modifications not supported

Type/Severity	Source	Description	Remedial Action
Critical	QoS	The system detected an internal error; The Specified modifier option is not supported.	Try again later, reset the QoS agent, or reset the unit.

Access element modifications not supported

Type/Severity	Source	Description	Remedial Action
Critical	QoS	The system detected an Internal error; The specified modifier option is not supported.	Try again later, reset the QoS agent or reset the unit.

Base action modifications not supported

Type/Severity	Source	Description	Remedial Action
Critical	QoS	The system detected an internal error; The specified modifier option is not supported.	Try again later, reset the QoS agent, or reset the unit.

Classifier block modifications not supported

Type/Severity	Source	Description	Remedial Action
Critical	QoS	The system detected an internal error; The specified modifier option is not supported.	Try again later, reset the QoS agent, or reset the unit.

Classifier component modifications not supported

Type/Severity	Source	Description	Remedial Action
Critical	QoS	The system detected an internal error; The specified modifier option is not supported.	Try again later, reset the QoS agent, or reset the unit.

Composite filter set addition failure comp filter set unknown

Type/Severity	Source	Description	Remedial Action
Critical	QoS	One of the components in the specified composite filter set does not exist.	Try again later, reset the QoS agent or reset the unit.

Comments? infodev@avaya.com

Composite filter set addition failure replication failure

Type/Severity	Source	Description	Remedial Action
Critical	QoS	The system failed to clone the composite filter member.	Try again later, reset the QoS agent, or reset the unit.

Composite filter set addition failure seed filter set unknown

Type/Severity	Source	Description	Remedial Action
Warning	QoS	The seed filter for the specified composite filter set does not exist.	Try again later, reset the QoS agent or reset the unit.

Composite filter set creation failure replication failure

Type/Severity	Source	Description	Remedial Action
Critical	QoS	The system failed to clone the filter set.	Try again later, reset the QoS agent, or reset the unit.

Composite filter set creation failure seed filter set unknown

Type/Severity	Source	Description	Remedial Action
Critical	QoS	The seed filter for the specified composite filter set does not exist.	Try again later, reset the QoS agent or reset the unit.

Composite filter set deletion failure comp filter set unknown

Type/Severity	Source	Description	Remedial Action
Critical	QoS	One of the components in the specified composite filter set does not exist.	Try again later, reset the QoS agent, or reset the unit.

Composite filter set deletion failure seed filter set unknown

Type/Severity	Source	Description	Remedial Action
Critical	QoS	The seed filter for the specified composite filter set does not exist.	Try again later, reset the QoS agent, or reset the unit.

CoS shaping modifications not supported

Type/Severity	Source	Description	Remedial Action
Critical	QoS	The system detected an internal error; The specified modifier option is not supported.	Try again later, reset the QoS agent, or reset the unit.

Count action modifications not supported

Type/Severity	Source	Description	Remedial Action
Critical	QoS	The system detected an internal error; The specified modifier option is not supported.	Try again later, reset the QoS agent or reset the unit.

Comments? infodev@avaya.com

Data model version attribute value not supported

Type/Severity	Source	Description	Remedial Action
Critical	QoS	Data versions 1 and 2 are currently supported in the system.	Try again later, reset the QoS agent or reset the unit.

DSCP mapping modifications not supported

Type/Severity	Source	Description	Remedial Action
Critical	QoS	The system detected an internal error; The specified modifier option is not supported.	Try again later, reset the QoS agent or reset the unit.

Filter manager internal error encountered

Type/Severity	Source	Description	Remedial Action
Critical	QoS	Internal filter manager error.	Try again later, reset the QoS agent or reset the unit.

Filter manager request parameter invalid

Type/Severity	Source	Description	Remedial Action
Critical	QoS	Invalid parameter detected during processing on the filter manager level.	Try again later, reset the QoS agent or reset the unit.

Incompatible data model version values (referenced clfr data)

Type/Severity	Source	Description	Remedial Action
Critical	QoS	The data model version of the classifier is unknown.	Try again later, reset the QoS agent or reset the unit.

Incompatible data model version values (referenced meter data)

Type/Severity	Source	Description	Remedial Action
Critical	QoS	The data model version of the meter is unknown	Try again later, reset the QoS agent or reset the unit.

Inconsistent classifier component (clfr comp#) state detected

Type/ Severity	Source	Description	Remedial Action
Critical	QoS	Unable to commit changes because of an invalid/ inconsistent state.	Try again later, reset the QoS agent or reset the unit.

Interface action extension identifier invalid

Type/Severity	Source	Description	Remedial Action
Critical	QoS	The interface action extension identifier is invalid.	Enter a valid interface action extension.

Comments? infodev@avaya.com

Interface action modifications not supported

Type/Severity	Source	Description	Remedial Action
Critical	QoS	The system detected an internal error; The specified modifier option not supported.	Try again later, reset the QoS agent, or reset the unit.

Interface application modifications not supported

Type/Severity	Source	Description	Remedial Action
Critical	QoS	The system detected an internal error; The specified modifier option is not supported.	Try again later, reset the QoS agent, or reset the unit.

Interface assignment modifications not supported

Type/Severity	Source	Description	Remedial Action
Critical	QoS	The system detected an internal error; The specified modifier option is not supported.	Try again later, reset the QoS agent, or reset the unit.

Interface queue modifications not supported

Type/Severity	Source	Description	Remedial Action
Critical	QoS	The system detected an internal error; the specified modifier option is not supported.	Try again later, reset the QoS agent or reset the unit.

Interface shaping modifications not supported

Type/Severity	Source	Description	Remedial Action
Critical	QoS	The system detected an Internal error; specified modifier option not supported.	Try again later, reset the QoS agent, or reset the unit.

Invalid classifier ID specified

Type/Severity	Source	Description	Remedial Action
Critical	QoS	Unable to find the specified classifier ID in the Filter Manager database.	Enter a valid classifier ID or if you are sure it exists try reseting the QoS agent or the unit.

Invalid classifier reference (unknown class)

Type/Severity	Source	Description	Remedial Action
Critical	QoS	There are 30 supported classes, check documentation for a full support class description.	Specify a valid classifier class.

Invalid datapath identifier specified

Type/Severity	Source	Description	Remedial Action
Critical	QoS	Invalid/Unknown datapath identifier detected. Internal Filter Manager error.	Try again later, reset the QoS agent or reset the unit.

Comments? infodev@avaya.com

Invalid master block member value specified

Type/Severity	Source	Description	Remedial Action
Critical	QoS	The master block member value can only have two values: True or False.	Try again later, reset the QoS agent or reset the unit.

Invalid option specified for BcastFrames attribute

Type/Severity	Source	Description	Remedial Action
Critical	QoS	BcastFrames attribute must be true or false. QPA internal error.	Try again later, reset the QoS agent or reset the unit.

Invalid option specified for KnownIpMcast attribute

Type/Severity	Source	Description	Remedial Action
Critical	QoS	KnownIpMcast attribute must be true or false. QPA internal error.	Try again later, reset the QoS agent or reset the unit.

Invalid option specified for KnownMcastFrames attribute

Type/Severity	Source	Description	Remedial Action
Critical	QoS	KnownMcastFrames attribute must be true or false. QPA internal error.	Try again later, reset the QoS agent or reset the unit.

Invalid option specified for KnownNonIpMcast attribute

Type/ Severity	Source	Description	Remedial Action
Critical	QoS	KnownNonIpMcast attribute must be true or false. QPA internal error.	Try again later, reset the QoS agent or reset the unit.

Invalid option specified for KnownUcastFrames attribute

Type/Severity	Source	Description	Remedial Action
Critical	QoS	KnownUcastFrames attribute must be true or false. QPA internal error.	Try again later, reset the QoS agent or reset the unit.

Invalid option specified for NonIpPkt attribute

Type/Severity	Source	Description	Remedial Action
Critical	QoS	NonIpPkts attribute must be true or false. QPA internal error.	Try again later, reset the QoS agent or reset the unit.

Invalid option specified for UnknownMcastFrames attribute

Type/Severity	Source	Description	Remedial Action
Critical	QoS	UnknownMcastFrames attribute must be true or false. QPA internal error.	Try again later, reset the QoS agent or reset the unit.

Comments? infodev@avaya.com

Invalid option specified for UnknownNonIpMcast attribute

Type/Severity	Source	Description	Remedial Action
Critical	QoS	UnknownNonIpMcast attribute must be true or false. QPA internal error.	Try again later, reset the QoS agent or reset the unit.

Invalid option specified for UnknownUcastFrames attribute

Type/Severity	Source	Description	Remedial Action
Critical	QoS	UnknownUcastFrames attribute must be true or false. QPA internal error.	Try again later, reset the QoS agent or reset the unit.

Invalid resetToDefaults value specified

Type/Severity	Source	Description	Remedial Action
Critical	QoS	ResetToDefaults must be “true” when trying to reset the QoS agent. This also goes for the partial reset.	Try again later or reset the unit.

Invalid unknown access assignment entry state encountered (entry state)

Type/Severity	Source	Description	Remedial Action
Critical	QoS	Unable to make changes because of an invalid or inconsistent state.	Try again later, reset the QoS agent, or reset the unit.

Invalid unknown access element entry state encountered (entry state)

Type/Severity	Source	Description	Remedial Action
Critical	QoS	Unable to make any changes due to of the invalid or inconsistent state.	Try again later, reset the QoS agent or reset the unit.

Invalid unknown action entry state encountered (entry state)

Type/Severity	Source	Description	Remedial Action
Critical	QoS	Unable to make changes because of an invalid/ inconsistent action entry state.	Try again later, reset the QoS agent or reset the unit.

Invalid unknown classifier block entry state encountered (entry state)

Type/ Severity	Source	Description	Remedial Action
Critical	QoS	Unable to make changes because of an invalid/ inconsistent state.	Try again later, reset the QoS agent or reset the unit.

Invalid unknown CoS shaping entry state encountered (entry state)

Type/Severity	Source	Description	Remedial Action
Critical	QoS	Unable to make changes because of an invalid or inconsistent state.	Try again later, reset the QoS agent or reset the unit.

Comments? infodev@avaya.com

Invalid unknown DSCP mapping entry state encountered (entry state)

Type/ Severity	Source	Description	Remedial Action
Critical	QoS	Unable to make changes because of an invalid/ inconsistent DSCP mapping entry state.	Try again later, reset the QoS agent or reset the unit.

Invalid unknown entry state (class class#) encountered (entry state)

Type/Severity	Source	Description	Remedial Action
Critical	QoS	Unable to make the changes because of an invalid/inconsistent state.	Try again later, reset the QoS agent, or reset the unit.

Invalid unknown interface action entry state encountered (entry state)

Type/Severity	Source	Description	Remedial Action
Critical	QoS	Unable to make changes because of an invalid state.	Try again later, reset the QoS agent or reset the unit.

Invalid/unknown interface app entry state encountered (<entry state>)

Type/Severity	Source	Description	Remedial Action
Critical	QoS	Unable to make the changes because of an	Try again later, reset the QoS agent, or reset the unit.

Type/Severity	Source	Description	Remedial Action
		invalid or inconsistent state.	

Invalid unknown interface assignment entry state encountered (entry state)

Type/Severity	Source	Description	Remedial Action
Critical	QoS	Unable to make changes because of an invalid/ inconsistent state.	Try again later, reset the QoS agent or reset the unit.

Invalid unknown interface queue entry state encountered (entry state)

Type/Severity	Source	Description	Remedial Action
Critical	QoS	Unable to make changes because of an invalid/ inconsistent interface queue entry state.	Try again later, reset the QoS agent or reset the unit.

Invalid unknown interface shaping entry state encountered (entry#)

Type/Severity	Source	Description	Remedial Action
Critical	QoS	Unable to make changes because of an invalid or inconsistent state.	Try later, reset the QoS agent or reset the unit.

Comments? infodev@avaya.com

Invalid unknown IP filter entry state encountered (entry state)

Type/Severity	Source	Description	Remedial Action
Critical	QoS	Unable to make changes because of an invalid/ inconsistent state.	Try again later, reset the QoS agent or reset the unit.

Invalid unknown Layer 2 filter entry state encountered (entry state)

Type/Severity	Source	Description	Remedial Action
Critical	QoS	Unable to make changes because of an invalid/ inconsistent state.	Try again later, reset the QoS agent or reset the unit.

Invalid unknown meter entry state encountered (entry state)

Type/Severity	Source	Description	Remedial Action
Critical	QoS	Unable to make changes because of an invalid/ inconsistent state.	Try again later, reset the QoS agent or reset the unit.

Invalid unknown policy entry state encountered (entry state)

Type/Severity	Source	Description	Remedial Action
Critical	QoS	Unable to make changes because of an invalid/ inconsistent state.	Try again later, reset the QoS agent or reset the unit.

Invalid unknown queue set assignment entry state encountered (entry state)

Type/Severity	Source	Description	Remedial Action
Critical	QoS	Unable to make changes because of an invalid/ inconsistent state.	Try again later, reset the QoS agent or reset the unit.

Invalid unknown queue shaping entry state encountered (entry state)

Type/Severity	Source	Description	Remedial Action
Critical	QoS	Unable to make changes because of an invalid/ inconsistent state.	Try again later, reset the QoS agent or reset the unit.

Invalid unknown queuing discipline enum specified (queuing discipline)

Type/Severity	Source	Description	Remedial Action
Critical	QoS	Only the following queuing disciplines are valid: FIFO, Priority Queuing, Fair Queuing, Weighted Fair Queuing and Weighted Round Robin Queuing.	Enter a valid/supported queuing discipline.

Comments? infodev@avaya.com

Invalid unknown role combination entry state encountered (entry state)

Type/Severity	Source	Description	Remedial Action
Critical	QoS	Unable to make changes because of an invalid/ inconsistent role combination state.	Try again later, reset the QoS agent or reset the unit.

Invalid unknown System filter entry state encountered (entry state)

Type/Severity	Source	Description	Remedial Action
Critical	QoS	Invalid entry state detected. Unable to commit changes.	Try again later, reset the QoS agent or reset the unit.

Invalid unknown token bucket entry state encountered (entry state)

Type/Severity	Source	Description	Remedial Action
Critical	QoS	Unable to make changes because of an invalid/ inconsistent state.	Try again later, reset the QoS agent or reset the unit.

Invalid unknown user policy entry state encountered (entry state)

Type/Severity	Source	Description	Remedial Action
Critical	QoS	Unable to make the changes because of an invalid or inconsistent state.	Try again later, reset the QoS agent, or reset the unit.

Invalid unknown 802.1p user priority mapping entry state (entry state)

Type/Severity	Source	Description	Remedial Action
Critical	QoS	Unable to make changes because of an invalid/ inconsistent 802.1p user priority state.	Try again later, reset the QoS agent or reset the unit.

IP classifier modifications not supported

Type/Severity	Source	Description	Remedial Action
Critical	QoS	The system detected an internal error; The specified modifier option not supported.	Try again later, reset the QoS agent or reset the unit.

Issue detected restoring QPA data from NV (class class#)

Type/Severity	Source	Description	Remedial Action
Critical	QoS	Unable to restore the QPA data from NVRAM (possible corrupt table(s)).	Reset the QoS agent or reset the unit.

Issues detected with QoS operational mode disable (ifcs# ifcs)

Type/Severity	Source	Description	Remedial Action
Critical	QoS	Unable to make changes (disable QoS) because of the specified interface configuration.	Check log for possible related details on the issue for and remove the conflicting configurations.

Comments? infodev@avaya.com

Issues detected with QoS operational mode enable (ifcs# ifcs)

Type/Severity	Source	Description	Remedial Action
Critical	QoS	Unable to make changes (enable QoS) because of the specified interface configuration.	Check log for possible related details on the issue and remove the conflicting configurations.

Layer 2 classifier modifications not supported

Type/Severity	Source	Description	Remedial Action
Critical	QoS	The system detected an internal error; The specified modifier option not supported.	Try again later, reset the QoS agent or reset the unit.

Meter modifications not supported

Type/Severity	Source	Description	Remedial Action
Critical	QoS	The system detected an internal error; The specified modifier option not supported.	Try again later, reset the QoS agent or reset the unit.

Modify the pattern data or use the correct data format

Type/Severity	Source	Description	Remedial Action
Critical	QoS	UnknownIpMcast attribute must be true or false. QPA internal error.	Try again later, reset the QoS agent or reset the unit.

Policy modifications not supported

Type/Severity	Source	Description	Remedial Action
Critical	QoS	The system detected an Internal error; The specified modifier option not supported.	Try again later, reset the QoS agent or reset the unit.

Post-join policy installation issue detected (ifc ifc#)

Type/Severity	Source	Description	Remedial Action
Critical	QoS	Unable to configure policies after a join stack event.	Try again or check stack health. Further conclusions can be drawn is this message appears either on base, non-base, all or some units in stack.

Potential inconsistent access elem state (Undo fail) detected

Type/Severity	Source	Description	Remedial Action
Critical	QoS	The system detected inconsistent access element state on the non base unit.	Try again later, reset the QoS agent, or reset the unit.

Potential inconsistent block state (Undo fail) detected

Type/Severity	Source	Description	Remedial Action
Critical	QoS	Inconsistent block state detected on non base unit.	Try again later, reset the QoS agent or reset the unit.

Comments? infodev@avaya.com

Queue set assignment modifications not supported

Type/Severity	Source	Description	Remedial Action
Critical	QoS	The system detected an Internal error; The specified modifier option not supported.	Try again later, reset the QoS agent or reset the unit.

Queue shaping modifications not supported

Type/Severity	Source	Description	Remedial Action
Critical	QoS	The system detected an internal error; The specified modifier option not supported.	Try again later, reset the QoS agent or reset the unit.

Resource alloc event timeout (tgt all apps except QoS Agent rcv event)

Type/Severity	Source	Description	Remedial Action
Critical	QoS	Filter Manager failed to allocate the necessary resources in time.	Reset the unit.

Role combination modifications not supported

Type/Severity	Source	Description	Remedial Action
Critical	QoS	The system detected an internal error; The specified modifier option not supported.	Try again later, reset the QoS agent or reset the unit.

Specified filter information not found

Type/Severity	Source	Description	Remedial Action
Critical	QoS	Failed to find the corresponding classifier in the datapath filter manager table.	Check that the entry queried exists, if so try reseting the QoS agent or the unit.

Specified filter manager resource invalid

Type/Severity	Source	Description	Remedial Action
Critical	QoS	Filter manager detected an invalid unit.	Try again later, reset the QoS agent or reset the unit.

Specified filter manager resource uninitialized

Type/Severity	Source	Description	Remedial Action
Critical	QoS	Unable to initialize the resource support.	Reset the unit.

Specified policy identifier (cookie) invalid

Type/Severity	Source	Description	Remedial Action
Critical	QoS	Filter Manager was unable to find the corresponding cookie for the specified policy.	Try again later, reset the QoS agent or reset the unit.

Comments? infodev@avaya.com

System classifier modifications not supported

Type/Severity	Source	Description	Remedial Action
Critical	QoS	The system detected an internal error; The specified modifier option not supported.	Try again later, reset the QoS agent or reset the unit.

Token bucket modifications not supported

Type/Severity	Source	Description	Remedial Action
Critical	QoS	The system detected an internal error; The specified modifier option not supported.	Try again later, reset the QoS agent or reset the unit.

Unable to complete requested access asgn system operation (oper type)

Type/Severity	Source	Description	Remedial Action
Critical	QoS	The system failed to enable or disable the access assignment on the base or non-base unit (in the stack).	Check log for related details on the issue. Try again later, reset the QoS agent, or reset the stack.

Unable to complete requested policy system operation (operation type)

Type/Severity	Source	Description	Remedial Action
Critical	QoS	The operation failed either on base or on non-base unit.	Try again later, reset the QoS agent, reset the unit or check stack health.

Unable to compress specified policy criteria

Type/Severity	Source	Description	Remedial Action
Critical	QoS	Unable to compress the rule and/or mask for the specified filter. Filter Manager internal error.	Try again later, reset the QoS agent or reset the unit.

Unable to create action for access element

Type/Severity	Source	Description	Remedial Action
Critical	QoS	Creation of action for the specified access element failed.	Try again later, reset the QoS agent or reset the unit.

Unable to create classifier block entry for access element

Type/Severity	Source	Description	Remedial Action
Critical	QoS	Creation of the classifier block entry failed.	Try again later, reset the QoS agent or reset the unit.

Unable to create classifier component entry for access element

Type/Severity	Source	Description	Remedial Action
Critical	QoS	Creation of the classifier component entry failed.	Try again later, reset the QoS agent or reset the unit.

Comments? infodev@avaya.com

Unable to create DS MF classifier for access element

Type/Severity	Source	Description	Remedial Action
Critical	QoS	DS(IP) MF Classifier creation failed.	Try again later, reset the QoS agent or reset the unit.

Unable to create L2 MF classifier for access element

Type/Severity	Source	Description	Remedial Action
Critical	QoS	Creation of the L2 MF classifier failed.	Try again later, reset the QoS agent or reset the unit.

Unable to install access element - component creation issue

Type/Severity	Source	Description	Remedial Action
Critical	QoS	The Access element installation failed.	Try again later, reset the QoS agent or reset the unit.

Unable to locate corresponding DS L2 access elements

Type/Severity	Source	Description	Remedial Action
Critical	QoS	The corresponding DS(IP)/L2 classifier(s) does not exist.	Try again later, reset the QoS agent or reset the unit.

Unknown access assignment entry specified (entry#)

Type/Severity	Source	Description	Remedial Action
Critical	QoS	Internal QPA error, the access assignment entry does not exist.	Try again later, reset the QoS agent, or reset the unit.

Unknown access element entry specified (entry#)

Type/Severity	Source	Description	Remedial Action
Critical	QoS	The system detected an internal QPA error; The count action entry does not exist.	Try again later, reset the QoS agent or reset the unit.

Unknown action entry specified (entry#)

Type/Severity	Source	Description	Remedial Action
Critical	QoS	The system detected an internal QPA error; the action entry does not exist.	Try again later, reset the QoS agent or reset the unit.

Unknown classifier block entry specified (entry#)

Type/Severity	Source	Description	Remedial Action
Critical	QoS	The system detected an internal QPA error; The classifier component entry does not exist.	Try again later, reset the QoS agent or reset the unit.

Comments? infodev@avaya.com

Unknown classifier component entry specified (entry#)

Type/Severity	Source	Description	Remedial Action
Critical	QoS	The system detected an internal QPA error; The classifier component entry does not exist.	Try again later, reset the QoS agent or reset the unit.

Unknown CoS shaping entry specified (entry# CoS)

Type/Severity	Source	Description	Remedial Action
Critical	QoS	The system detected an Internal QPA error; The interface shaping entry does not exist.	Try again later, reset the QoS agent or reset the unit.

Unknown count action entry specified (entry#)

Type/Severity	Source	Description	Remedial Action
Critical	QoS	The system detected an internal QPA error; The count action entry does not exist.	Try again later, reset the QoS agent or reset the unit.

Unknown DSCP mapping entry specified (entry#)

Type/Severity	Source	Description	Remedial Action
Critical	QoS	The system detected an internal QPA error; The DSCP mapping entry does not exist.	Try again later, reset the QoS agent or reset the unit.

Unknown entry (class class#) specified (entry#)

Type/Severity	Source	Description	Remedial Action
Critical	QoS	The system detected an internal QPA error; The specified entry does not exist.	Try again later, reset the QoS agent, or reset the unit.

Unknown incompatible token bucket reference specified

Type/Severity	Source	Description	Remedial Action
Critical	QoS	Referenced token bucket not found.	Enter an existing/compatible token bucket.

Unknown interface application entry specified (entry#)

Type/ Severity	Source	Description	Remedial Action
Critical	QoS	The system detected an internal QPA error; The interface application entry does not exist.	Try again later, reset the QoS agent, or reset the unit.

Unknown interface assignment entry specified (entry#)

Type/Severity	Source	Description	Remedial Action
Critical	QoS	The system detected an internal QPA error; The interface assignment entry does not exist.	Try again later, reset the QoS agent or reset the unit.

Comments? infodev@avaya.com

Unknown interface queue entry specified (ifc queue id)

Type/Severity	Source	Description	Remedial Action
Critical	QoS	The system detected an internal QPA error; The interface queue entry does not exist.	Try again later, reset the QoS agent or reset the unit.

Unknown interface shaping entry specified (entry#)

Type/Severity	Source	Description	Remedial Action
Critical	QoS	The system detected an iternal QPA error; The interface shaping entry does not exist.	Try again later, reset the QoS agent or reset the unit.

Unknown IP classifier entry specified (entry#)

Type/Severity	Source	Description	Remedial Action
Critical	QoS	The system detected an internal QPA error; The IP classifier does not exist.	Try again later, reset the QoS agent or reset the unit.

Unknown Layer 2 classifier entry specified (entry#)

Type/Severity	Source	Description	Remedial Action
Critical	QoS	The system detected an internal QPA error; The l2 classifier does not exist.	Try again later, reset the QoS agent or reset the unit.

Unknown meter entry specified (entry#)

Type/Severity	Source	Description	Remedial Action
Critical	QoS	The system detected an internal QPA error; The meter component entry does not exist.	Try again later, reset the QoS agent or reset the unit.

Unknown policy entry specified (entry#)

Type/ Severity	Source	Description	Remedial Action
Critical	QoS	The system detected an internal QPA error; The classifier component entry does not exist.	Try again later, reset the QoS agent or reset the unit.

Unknown queue set assignment entry specified (entry#)

Type/Severity	Source	Description	Remedial Action
Critical	QoS	The system detected an internal QPA error; The queue set does not exist.	Try again later, reset the QoS agent or reset the unit.

Unknown queue shaping entry specified (entry# queue)

Type/Severity	Source	Description	Remedial Action
Critical	QoS	The system detected an internal QPA error; The count action entry does not exist.	Try again later, reset the QoS agent or reset the unit.

Comments? infodev@avaya.com

Unknown role combination entry specified (role comb id)

Type/Severity	Source	Description	Remedial Action
Critical	QoS	The system detected an internal QPA error; The role combination entry does not exist.	Try again later, reset the QoS agent or reset the unit.

Unknown System classifier entry specified (entry#)

Type/Severity	Source	Description	Remedial Action
Critical	QoS	The system detected an Internal QPA error; the system classifier does not exist.	Try again later, reset the QoS agent or reset the unit.

Unknown token bucket entry specified (entry#)

Type/Severity	Source	Description	Remedial Action
Critical	QoS	The system detected an internal QPA error; The token bucket does not exist.	Try again later, reset the QoS agent or reset the unit.

Unknown unsupported RowStatus specified

Type/Severity	Source	Description	Remedial Action
Critical	QoS	The status is unknown or unsupported for the current entry. Valid statuses are (the supported ones depend on the QoS component): active, create and go, create and wait, destroy, not in service, not ready.	Try again later, reset the QoS agent or reset the unit.

Unknown user policy entry specified (entry#)

Type/ Severity	Source	Description	Remedial Action
Critical	QoS	The system detected an internal QPA error; The user policy entry does not exist.	Try again later, reset the QoS agent, or reset the unit.

Unknown 802.1p user priority mapping entry specified (entry#)

Type/Severity	Source	Description	Remedial Action
Critical	QoS	The system detected an internal QPA error; The 802.1p user priority mapping entry does not exist.	Try again later, reset the QoS agent or reset the unit.

Unsupported IPv4 Options value specified

Type/Severity	Source	Description	Remedial Action
Critical	QoS	Invalid IPv4 option detected.	Try again later, reset the QoS agent or reset the unit.

User policy modifications not supported

Type/Severity	Source	Description	Remedial Action
Critical	QoS	The system detected an internal error; The specified modifier option not supported.	Try again later, reset the QoS agent, or reset the unit.

Comments? infodev@avaya.com

QoS warning messages

Access assignment modification support limited

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Access assignment entries under system control may be deleted but not modified. The same goes for templates.	Create a different access assignment entry with the wanted parameters.

Access assignment name contains unacceptable characters

Type/ Severity	Source	Description	Remedial Action
Serious	QoS	Only printable characters are allowed.	Enter valid characters for the access element block label.

Access assignment name length outside of acceptable limits

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The maximum length for the access assignment name is 16.	Enter an access assignment label within the limit.

Access assignment name not acceptable - reserved

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The label is reserved in the system.	Enter a different label.

Access assignment template still in use (siblings active)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Cannot delete an access assignment entry if it has one or more active siblings in use.	Remove the sibling(s) first.

Access element block label contains unacceptable characters

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Only printable characters are allowed.	Enter valid characters for the access element block label.

Access element block label length outside of acceptable limits

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The maximum length for the access element block name is 16.	Enter a smaller access element block label.

Access element cluster count (cluster count) exceeds limit (cluster limit)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The cluster limit of the access element depends on the target hardware platform.	Check the documentation for the maximum number of access elements allowed.

Comments? infodev@avaya.com

Access element cluster is referenced (addition prohibited)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The access-list can not be modified if it is currently referenced (assigned).	Remove the referee before requesting any modifications.

Access element cluster is referenced (deletion prohibited)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Access element can not be removed if it is currently referenced.	Remove the conflicting element first.

Access element name contains unacceptable characters

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Only printable characters are allowed.	Enter valid characters for the access element's label.

Access element name length outside of acceptable limits

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The maximum length for the access element name is 16.	Enter a smaller access element label.

Access element name not acceptable - reserved

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The label is reserved in the system.	Enter a different label.

Attempt to create an element that already exists (prohibited)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	An entry with the same characteristics already exists in the system.	Remove the existing entry if necessary.

Attempt to delete modify non-existing element (prohibited)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	You cannot remove or modify an inexistent element.	If this is a modification attempt create a new element.

Attempt to manipulate system-owned interface (prohibited)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Modification of the system-owned interfaces is prohibited.	Enter a different interface index.

Comments? infodev@avaya.com

Attempt to manipulate user policy data rejected (disabled)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	All user based policy data modifications are prohibited when the UBP support is disabled.	Enable the UPB support.

Base action entry referenced by clfr block (deletion prohibited)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Cannot delete a base action if it's referenced by a classifier block.	Remove the classifier block first.

Base action entry referenced by meter (deletion prohibited)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Cannot delete a base action if it's referenced in a meter.	Remove the meter first.

Base action entry referenced by policy (deletion prohibited)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Cannot delete a base action if it's referenced by a policy.	Remove the policy first.

Base action modification prohibited due to action usage

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Cannot modify a base action if it's in use.	Remove the QoS entries that are using the base action first.

Base action extension identifier invalid

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The specified base action extension identifier is invalid	Enter a valid base action extension identifier.

Buffer configuration inconsistency detected (local buffer conf stack buffer conf)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The buffering configuration is not the same on all units in stack.	Try again later, reset the QoS agent or reset the unit.

Classifier block component set ID out-of-range (clfr comp set ID)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Set ID must be between 1 and 55000.	Enter a valid classifier block component setID.

Comments? infodev@avaya.com

Classifier block number out-of-range (block#)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Classifier block number must be between 1 and 55000.	Enter a valid classifier block number.

Classifier block precedence value not supported

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Classifier block precedence range depends on the platform.	Check documentation and use a valid classifier block precedence or ignore option.

Classifier component set ID out-of-range (clfsr comp set ID)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Set ID must be between 1 and 55000.	Specify a valid set ID.

Classifier conflict (duplicate clfr data in block) detected

Type/Severity	Source	Description	Remedial Action
Serious	QoS	A classifier with the same characteristics already exists in the specified block.	Remove the existing classifier or use a different block.

Classifier content incompatible with target interface(s)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The classifier element options not supported by the specified interface(s).	Change the classifier content and try again or change the interface(s).

Classifier set block reference out-of-range (clfr setblock#)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Classifier set/block id must be between 1 and 55000.	Enter a valid classifier set/ block id.

Classifier type unknown

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The valid classifier types are individual and block.	Specify a valid classifier type.

Clfr content (system) incompatible with target interface(s)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The system classifier element options not supported by the specified interface(s).	Change the system classifier content and try again or change the interface(s).

Comments? infodev@avaya.com

Composite filter set addition failure data consistency issue

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The system detected inconsistent data; Following are the possible reasons: Filter set duplication, Conflicting MAC data (the same filter set cannot be added with or without MAC data).	Check the parameters, and resolve if any possible invalid values.

Composite filter set addition failure data invalid

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The system detected invalid data; Following are the possible reasons: Source MAC address and mask length with different values, Seed name must be specified, and within the limited length, Clone name must be specified, and within the limited length (0-16).	Check the parameters and resolve if any possible invalid values.

Composite filter set addition failure resources unavailable

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Unable to add any more members to the specified filter set as the resources are unavailable.	Check for and remove the resources that are not needed.

Composite filter set creation failure MAC data not allowed

Type/Severity	Source	Description	Remedial Action
Serious	QoS	MAC data is not allowed in the base composite filter set.	Remove the MAC data filter or classifier.

Composite filter set creation failure data invalid

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The system detected invalid data; Following are the possible reasons: Source MAC address and mask length with different values, Seed name must be specified; and within the limited length, Clone name must be specified, and within the limited length.	Check the parameters, and resolve if any possible invalid values.

Composite filter set deletion failure base set target invalid

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The base composite filter set is on target. The base composite filter set can not be deleted without destroying the entire composite filter set.	Remove the filter set dependencies if any before deleting the base filter set.

Comments? infodev@avaya.com

Composite filter set deletion failure data invalid

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The system detected invalid data; Following are the possible reasons: Source MAC address and mask length with different values, Seed name must be specified and within the limited length, Clone name must be specified and within the limited length (0-16).	Check the parameters and resolve, if any possible invalid values.

Composite filter set destruction failure data invalid

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The system detected invalid data detected; Following is the possible reason: The Clone name must be specified and within the limited length (0-16).	Check the parameters and resolve, if any possible invalid values.

Composite filter set membership limits exceeded

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The maximum number of composite members in a filter set is 16.	Enter at the most 16 composite members in a filter set.

Conflicting action sources detected

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Multiple actions specified from different sources (via policy match action, policy meter or classifier block) A combination of sources if prohibited.	Remove conflicts by using a single action source.

Conflicting master block member information detected

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Multiple master blocks detected.	Enter a single master block.

Conflicting policy role policy interface index data detected

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Both role and interface index were specified.	Enter either a role or an interface index.

CoS shaping not supported with specified interface

Type/ Severity	Source	Description	Remedial Action
Serious	QoS	The specified interface is unable to support the CoS shaping.	Enter a different interface.

Comments? infodev@avaya.com

Count action entry referenced by meter (deletion prohibited)

Type/ Severity	Source	Description	Remedial Action
Serious	QoS	Cannot delete a count action entry if it's referenced by a meter.	Remove the meter first.

Count action entry referenced by policy (deletion prohibited)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Cannot delete a count action if it's referenced by a policy.	Remove the policy first.

DAPP resources not available (unit unit#)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Some of the resources required are not available on all the interfaces.	Check for and remove unneeded resources.

DAPP with statistics tracking in use (QoS disable prohibited)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Cannot disable the QoS system if DAAP with tracking statistics is enable.	Disable DAAP or change it;s enabled state before disabling QoS.

Default ifc assignment failure port# port(s) ifc QoS-disabled

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Unable to set the specified port to it's default state.	Reset the QoS agent or reset the unit.

Destination MAC address and mask values out-of-sync

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The destination MAC address and mask do not correspond (at least one address bit not included in mask is set).	Modify the destination MAC address or mask.

Different classifier component masks keys in block detected

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Examines classifier criteria to determine whether the specified data is supported in the context of the target interface(s).	Use a compatible interface or change the conflicting filter criteria.

DSCP remarking not supported for IPv6 (green action)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Match action (green) containing DSCP remarking cannot be used on a filter with Ipv6 fields.	Enter a different match action or a different classifier.

Comments? infodev@avaya.com

DSCP remarking not supported for IPv6 (in-profile action)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	In-profile action containing DSCP remarking cannot be used on a filter with Ipv6 fields.	Enter a different in-profile action or a different classifier.

DSCP remarking not supported for IPv6 (match action)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Match action containing DSCP remarking cannot be used on a filter with Ipv6 fields.	Enter a different match action or a different classifier.

DSCP remarking not supported for IPv6 (non-match action)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Non-match action containing DSCP remarking cannot be used on a filter with Ipv6 fields.	Enter a different non-match action or a different classifier.

DSCP remarking not supported for IPv6 (out-of-profile action)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Out-of-profile action containing DSCP remarking cannot be used on a filter with Ipv6 fields.	Enter a different out-of-profile action or a different classifier.

DSCP remarking not supported for IPv6 (red action)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Match action (red) containing DSCP remarking cannot be used on a filter with Ipv6 fields.	Enter a different match action or a different classifier.

DSCP remarking not supported for IPv6 (yellow action)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Match action (yellow) containing DSCP remarking cannot be used on a filter with Ipv6 fields.	Enter a different match action or a different classifier.

Dst IP addr matching not supported with IP addr type data

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Filters with pattern matching (Dst IP) cannot be used with data of the IP address type .	Separate the conflicting elements into multiple filters.

Dst Layer 4 port min max values invalid (max must be = to min)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The maximum destination port must be bigger than the minimum destination port.	Correct destination port range limits.

Comments? infodev@avaya.com

Dst MAC addr matching not supported with address type data

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Destination MAC address matching and the address type matching is prohibited in the same classifier element.	Separate the conflicting elements into multiple filters.

Duplicate access asgn name type index detected (prohibited)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Multiple entries with the same name, type, or index are prohibited.	Enter a different name, type, index compared to the ones already installed in the system.

Duplicate classifier class values in set detected

Type/Severity	Source	Description	Remedial Action
Serious	QoS	A classifier with the same class already exists in the specified set-id.	Remove the existing classifier or use a different set-id.

Duplicate set values in block detected

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The specified set value already exists in classifier block.	Enter a different set value or remove the existing one.

Egress interface and egress mask are mutually exclusive

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Invalid egress mask.	Enter both options (egress unicast and egress non-unicast) with the same port.

Element enable prohibited. Please delete and re-enter data

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Request rejected as no underlying policies are configured.	Delete and re-enter valid data.

Element label contains unacceptable characters

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Only printable characters are allowed	Enter valid characters for the access element's label.

Element label length outside of acceptable limits (max 16 chars)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The maximum length for QoS labels if 16 characters.	Enter a smaller label in order for it to be accepted by the system.

Comments? infodev@avaya.com

Evaluation precedence conflict (Traffic Prof filter set data)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The system detected a Precedence conflict - multiple entries cannot occupy the same precedence on the same port.	Check for the available precedence, and remove the resources that are not needed if any.

Evaluation precedence conflict detected (UBP filter set data)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Unable to make the required changes.	Check the availability of resources on the specified port or use a different interface index.

Evaluation precedence value required but not specified

Type/Severity	Source	Description	Remedial Action
Serious	QoS	A precedence must be assigned to the access classifier (similar to the policy), else it cannot be installed on the interface.	Enter a specific or the next available precedence.

FCoE redirection default frame filter deletion failure detected

Type/Severity	Source	Description	Remedial Action
Serious	FCoE Redirect	Unable to delete installed FCoE Redirect policy data.	Toggle feature enable and retry.

FCoE redirection default frame filter installation failure detected

Type/Severity	Source	Description	Remedial Action
Serious	FCoE Redirect	Unable to install required FCoE Redirect policy data.	Toggle feature enable and retry.

FCoE redirection - egress interface issue detected (ifIndex %d)

Parameters	Type/Severity	Source	Description	Remedial Action
IfIndex	Serious	FCoE Redirect	Issue detected with interface used with FCoE Redirect.	Check status of identified interface.

FCoE redirection - egress trunk issue detected (trunk ID %d)

Parameters	Type/Severity	Source	Description	Remedial Action
Trunk ID	Serious	FCoE Redirect	Issue detected with trunk used with FCoE Redirect.	Check status of identified trunk.

Filter control block resources exhausted

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Not enough resources to create the specified filter control block.	Check for and remove unneeded resources.

Comments? infodev@avaya.com

Filter creation issue detected - in-profile action component

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Unable to create filter because of a conflicting in-profile action component.	Identify and remove the conflicting component(s).

Filter creation issue detected - match action component

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Unable to create filter because of a conflicting match action component.	Identify and remove the conflicting component(s).

Filter creation issue detected - metering component

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Unable to create filter because of a conflicting meter component.	Identify and remove the conflicting component(s).

Filter creation issue detected - non-match action component

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Unable to create filter because of a conflicting non-match action component.	Identify and remove the conflicting component(s).

Filter creation issue detected - out-of-profile action component

Type/ Severity	Source	Description	Remedial Action
Serious	QoS	Unable to create filter because of a conflicting out-of-profile action component.	Identify and remove the conflicting component(s).

Filter manager memory resources exhausted

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Not enough resources or inconsistent memory.	Check for and remove the unneeded resources.

Filter manager metering or policy rule space exhausted

Type/Severity	Source	Description	Remedial Action
Serious	QoS	There is no more space available for rule allocation.	Check for and remove unneeded resources.

Filter manager metering resources exhausted

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The filter manager meter support reached it's limit.	Check for and remove unneeded meters.

Comments? infodev@avaya.com

Filter manager statistics tracking resources exhausted

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The statistics tracking/ counter table is full.	Check for and remove unneeded statistics related entries.

Filter set requirements incompatible with target interface

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The requirements are not compatible with the target interface.	Enter a different interface or a compatible set of requirements.

First TrTCM Meter Index must be in range 1-5000

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The maximum valid index for the first TrTCM meter is 5000	Specify a valid index.

Flow ID filtering not supported for IPv4

Type/ Severity	Source	Description	Remedial Action
Serious	QoS	Flow ID is supported only for IPV6.	Enter a Ipv6 address or specify the address type (must be Ipv6).

Flow ID out-of-range (Flow ID)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Invalid flow ID specified.	Enter a flow ID between 0x00-0xfffff (1048575).

In-profile action contains conflicting data

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Unable to install the specified in-profile action, conflicting data detected.	Identify conflicts and separate them into different in-profile actions.

Ifc app modification issue (inconsistent default gateway data)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Modification is prohibited as an inconsistent default gateway data is detected.	Remove the entry and add a new one with the modified default gateway value.

Ifc app modification issue (inconsistent DHCP server data)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Modification is not allowed as the system detected inconsistent DHCP server data.	Remove the entry and add a new one to the modified DHCP server.

Comments? infodev@avaya.com

Ifc app modification issue (inconsistent ifType data)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Modification is not allowed as an inconsistent interface type data is detected.	Remove the entry and add a new one with the modified interface type data.

Ifc app support not currently available on interface (ifc#)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Interface application support is not available on the specified interface as it is incompatible or disabled.	Enter a different interface index.

Ifc assignment issue - prec conflict (policy policy# disabled)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The interface assignment change needs to install a policy on a precedence that is already occupied by a different one, as a result the conflicting policy was disabled.	Analyze the conflict and choose an appropriate solution (the interface assignment or the policy).

Inadequate resources available for application policy criteria

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The resources potentially consumed by a legacy filter set are not available on the specified interface (on the base or the non-base unit).	Check log for the possible related details on the issue. Check the available resources.

Incompatible base action extension specified

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The storage types are not compatible. For example only system-level entries can reference other system-level entries.	Check the documentation if necessary and use compatible entries.

Incompatible classifier reference (agent-defined clfr)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	It's forbidden to reference an system/agent defined classifier element.	Create a similar user defined classifier element.

Incompatible in-profile action (trusted ifc)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The specified in-profile action is not supported on the associated interface type (trusted).	Enter a different in-profile action or change interface group assignment.

Incompatible in-profile action (unrestricted ifc)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The specified in-profile action is not supported on the associated interface type (unrestricted).	Enter a different in-profile action or change interface group assignment.

Comments? infodev@avaya.com

Incompatible in-profile action (untrusted ifc)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The specified in-profile action is not supported on the associated interface type (untrusted).	Enter a different in-profile action or change interface group assignment.

Incompatible match action (unrestricted ifc)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The specified action is not supported on the associated interface type (unrestricted).	Enter a different action or change interface group assignment.

Incompatible match action (untrusted ifc)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The specified action is not supported on the associated interface type (untrusted).	Enter a different action or change interface group assignment.

Incompatible non-match action (unrestricted ifc)

Type/ Severity	Source	Description	Remedial Action
Serious	QoS	The specified non-match action is not supported on the associated interface type (unrestricted).	Enter a different non-match action or change interface group assignment.

Incompatible non-match action (trusted ifc)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The specified non-match action is not supported on the associated interface type (trusted)	Enter a different non-match action or change interface group assignment.

Incompatible non-match action (unrestricted ifc)

Type/ Severity	Source	Description	Remedial Action
Serious	QoS	The specified non-match action is not supported on the associated interface type (unrestricted).	Enter a different non-match action or change interface group assignment.

Incompatible non-match action (untrusted ifc)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The specified non-match action is not supported on the associated interface type (untrusted).	Enter a different non-match action or change interface group assignment.

Incompatible out-of-profile action (trusted ifc)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The specified out-of-profile action is not supported on the associated interface type (trusted).	Enter a different out-of-profile action or change interface group assignment.

Comments? infodev@avaya.com

Incompatible out-of-profile action (unrestricted ifc)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The specified out-of-profile action is not supported on the associated interface type (unrestricted).	Enter a different out-of-profile action or change interface group assignment.

Incompatible out-of-profile action (untrusted ifc)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The specified out-of-profile action is not supported on the associated interface type (untrusted).	Enter a different out-of-profile action or change interface group assignment.

Incompatible StorageType specified (re classifier)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The policy and classifier have incompatible storage types. As a general rule only system-level entries can reference other system-level entries.	Enter a compatible classifier or create a new one.

Inconsistent action criteria detected across block members

Type/ Severity	Source	Description	Remedial Action
Serious	QoS	The action options within a block entry must be consistent. For instance you cannot specify an action and	Enter only an action or a meter across block.

Type/ Severity	Source	Description	Remedial Action
		a meter for a block in the same time.	

Inconsistent labels detected for members of same block

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The members of the same classifier-block must have the same label.	Enter the same label for all members.

Inconsistent labels detected for members of same set

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Entries of the same set must have the same labels.	Enter the same labels for all members in the set or separate the conflicting components into multiple sets.

Inconsistent MAC data detected across filter set members

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Inconsistent MAC data detected across the filter sets; Following are the possible reasons: Different users are on the same interface with different MAC data length, Different users on the same interface with the same MAC data source.	Check for and remove the possible MAC data conflicts.

Comments? infodev@avaya.com

Inconsistent metering criteria detected across block members

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Invalid metering option specified. QPA internal error.	Enter a valid meter or ignore option.

Inner VLAN ID filtering requires double tag

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Inner VLAN ID is used in double tagged packets.	Remove inner VLAN ID option or specify double tagged mode.

Inner VLAN ID min max values invalid (min VLAN ID ! max VLAN ID)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Max inner VLAN ID value must be bigger that min value.	Correct inner VLAN ID range limits.

Insufficient HW resources to support port role association

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Not all the resources required for the interface assignment change are available.	Check for conflicts and remove the un-needed resources if any.

Insufficient policy space available to support access assignment

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Not enough resources to support the policy installation on base or non-base unit.	Check the policy resource availability and try to remove any resources that are not needed.

Insufficient resources available to support policy installation

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Not all the resources required for the policy are available on the base or non-base unit(s).	Modify either the interfaces or the demanding resources.

Interface action entry referenced by base action

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Cannot modify or delete an interface action if it is referenced by a base action.	Remove the base action first.

Interface Application data in use (QoS disable prohibited)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Cannot disable the QoS system if there are Interface Applications in use.	Disable all the Interface Applications before disabling QoS.

Comments? infodev@avaya.com

Interface application Undo failure (app app#)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Unable to perform the “Undo” action due to the the specified interface application.	Check log for related details on the issue. Try again later, reset the QoS agent, or reset the stack.

Interface assignment failure - precedence conflict detected

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The interface assignment change needs to install a policy on a precedence already occupied by a different one.	Remove or disable if possible the conflicting policy.

Interface capabilities incompatible with policy data

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The policy and the specified interface have different version capabilities.	Enter either a compatible interface or adapt the policy to match the required interface.

Interface resources inadequate to support application enable

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The resources required for interface application support are not available on the specified interface.	Check log for related details on the issue, or use a different interface.

Interface shaping and CoS shaping conflict (same ifc specified)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Interface shaping and CoS shaping can not be applied to the same interface at the same time.	Enter different interfaces for the two shaping types.

Interface shaping and queue shaping conflict (same ifc specified)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Both Interface and queue shaping can not be applied to the one interface at the same time.	Enter different interfaces for the two shaping types.

Interface shaping not supported with specified interface

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The specified interface is unable to support the shaping.	Enter a different interface.

Interfaces QoS-disabled (port# on unit#) - restoration issue

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Failed to disable the Policy/ Interface.	Check for the conflicting entries, try again later, reset the QoS agent or reset the unit.

Comments? infodev@avaya.com

Invalid 802.1p user priority value specified (priority value)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The only valid user priorities values are between 0 and 7.	Specify a valid user priority.

Invalid access element type option specified

Type/Severity	Source	Description	Remedial Action
Serious	QoS	There are 4 supported access element types: ACL, APP, MMC, and UDC; Check through the documentation for further clarifications on the issue.	Remove the classifier block first.

Invalid access assignment type option specified

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The access assignment type option specified is invalid.	Check the documentation and use a supported access assignment type.

Invalid classifier reference

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The only valid classifiers type are: ip, l2 and system.	Specify a valid classifier type.

Invalid classifier reference (unknown incompatible set)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The referenced classifier set must exist prior to being used.	Enter an existing classifier set or create a new one.

Invalid classifier reference (unknown instance)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The referenced classifier element (ip, l2 or system) must exist prior to being used.	Enter an existing classifier element or create a new one.

Interface data out-of-sync in Policy and User Policy entries

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The interface data associated with the policy and the session must be the same.	Specify the same interface data.

Invalid DAPP state transition detected (prohibited)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Can only move between disabled and enabled, not between different enable modes.	Disable DAPP before changing the enabled state.

Comments? infodev@avaya.com

Invalid destination MAC address length specified

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Destination MAC address length is bigger than 6.	Specify a valid MAC address.

Invalid destination MAC address mask length specified

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Destination MAC address mask length is bigger than 6.	Specify a valid MAC address mask.

Invalid DSCP value specified (DSCP value)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The valid DSCP values are between 0 and 63.	Enter a valid DSCP value in the range specified.

Invalid drop precedence value specified (precedence)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Valid drop precedence values are low and high.	Specify a valid drop precedence value.

Invalid egress interface specified (ifc#)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The interface index does not exist.	Check the platform's/stack's port range and use a valid interface index.

Invalid egress interface type specified (<ifc type>)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Interface can not be associated with action specifications(prohibited).	Enter a different port.

Invalid egress mask value specified

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The egress mask must be either null or 64 in length.	Specify a valid egress mask.

Invalid EtherType value specified (Ether Type 0xXXXX)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	EtherType must be between 0x0-0xFFFF.	Specify an EtherType value between 0x0-0xFFFF.

Comments? infodev@avaya.com

Invalid expired session data specified

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The session data provided does not exist or has expired.	Specify a current session data.

Invalid filter set priority value detected

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The filter set priority must be within 1 to 255.	Check the log for related details on the issue. Try again later, reset the QoS agent, or reset the stack

Invalid track statistics value specified

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The only valid tracking statistics values are disabled, individual and aggregate.	Assign a valid tracking statistics value.

Invalid interface found in egress mask (egrees mask bit#)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The Interface doesn't exist or is not supported.	Enter a different interface/ port number.

Invalid interface index data specified (ifc#)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The interface index not in range (1-1024).	Check unit/stack limitations.

Invalid interface index data specified (ifc index)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The interface index does not exist.	Check the port range of the platform or stack, and use a valid interface index.

Invalid interface index data (system-owned) specified

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Only system-owned policies can reference system-owned interfaces.	Enter an interface that is not system-owned.

Invalid IP destination address prefix detected

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The specified destination address prefix exceeds the maximum allowed for ipv4 addresses (32).	Enter the correct prefix.

Comments? infodev@avaya.com

Invalid IP source address prefix detected

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The specified source address prefix exceeds the maximum allowed for ipv4 addresses (32).	Enter the correct prefix.

Invalid maximum inner VLAN ID value specified (VLAN ID)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The maximum inner VLAN ID is 4094 .	Specify a valid VLAN ID value.

Invalid minimum inner VLAN ID value specified (VLAN ID)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The inner VLAN ID must be greater than 1.	Enter an VLAN ID greater than 1.

Invalid maximum VLAN ID value specified (VLAN ID)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The maximum VLAN ID is 4094.	Specify a valid VLAN ID value.

Invalid metering data (bucket size) specified for interface(s)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The current metering bucket size is not supported on the current interface.	Change the target interface or modify the metering bucket size.

Invalid metering data (granularity) specified for interface(s)

Type/ Severity	Source	Description	Remedial Action
Serious	QoS	The metering granularity is not supported on the current interface.	Change the target interface or modify the metering granularity.

Invalid metering data (rate) specified for interface(s)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The metering rate is not supported on the current interface.	Change the target interface or modify the metering rate.

Invalid metering data (srTCM trTCM) specified for interface(s)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The metering type is not supported on the current interface.	Change the target interface or modify the metering type.

Comments? infodev@avaya.com

Invalid minimum VLAN ID value specified (VLAN ID)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The VLAN ID must be bigger than.	Enter an ID bigger than 1.

Invalid mix of IP address data (Dst IP type) in set detected

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Different filter criteria can be specified in the same classifier but they must be compatible. Conflict(s) detected when validating Dst IP/type data.	Separate the conflicting elements into multiple classifier sets.

Invalid mix of IP data (IPv4 IPv6) in set detected

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Different filter criteria can be specified in the same classifier but they must be compatible. IPv4 and Ipv6 data are mutually exclusive.	Separate the conflicting elements into multiple classifier sets.

Invalid mix of IP and non-IP data in set detected

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Even though different classifier element types can be specified in the same classifier they must be compatible. IP and non-IP data are mutually exclusive.	Separate the IP and non-IP pattern data in different classifier sets.

Invalid option specified for PatternIpVersion attribute

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Valid PatternIpVersion are non-ip, ipv4, ipv6.	Enter a valid version or remove option.

Invalid pattern data length (untagged format) specified

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Pattern data length does not correspond with the specified data format (untagged).	Modify the pattern data or use the correct data format.

Invalid pattern data string length specified

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Patter data string length must be between 0 and 128.	Specify a valid length.

Invalid pattern format data specified

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Supported formats: untagged, tagged or double tagged.	Specify a supported format data.

Comments? infodev@avaya.com

Invalid pattern position string length specified

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Patter position string length must be between 0 and 128.	Specify a valid length.

Invalid port detected in specified port mask

Type/Severity	Source	Description	Remedial Action
Serious	QoS	An unknown/invalid port was detected in the specified port mask.	Inspect the mask and remove the invalid port(s).

Invalid set drop precedence value specified

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The drop precedence can have two values, low or high.	Check the documentation if necessary and use a valid drop precedence value.

Invalid shaping data (bucket size) specified for interface(s)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The shaping bucket size is not supported on the current interface.	Change the target interface or modify the shaping bucket size.

Invalid shaping data (granularity) specified for interface(s)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The shaping granularity is not supported on the current interface.	Change the target interface or modify the shaping granularity.

Invalid shaping data (minimum rate granularity) specified

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The minimum shaping rate granularity is invalid or not supported.	Modify the minimum shaping rate granularity to a valid or supported value.

Invalid shaping data (minimum rate maximum rate) specified

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The limits of the shaping rate are not in order; the minimum rate must be lesser than the maximum rate.	Change the shaping rate limits.

Invalid shaping data (minimum rate) specified

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The minimum shaping rate is not supported on the current interface.	Change the target interface or modify the minimum shaping rate.

Comments? infodev@avaya.com

Invalid shaping data (rate) specified for interface(s)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The shaping rate is not supported on the current interface.	Change the target interface or modify the shaping rate.

Invalid source MAC address length specified

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Source MAC address length is greater than 6.	Specify a valid MAC address.

Invalid source MAC address mask length specified

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Source MAC address mask length is greater than 6.	Specify a valid MAC address mask.

Invalid statistics counter identification specified

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The statistics counter identifier provided is invalid.	Enter a valid statistics tracking identifier.

Invalid statistics tracking value

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Invalid policy tracking statistics. The supported	Specify a supported policy tracking statistics.

Type/Severity	Source	Description	Remedial Action
		types are: individual aggregate or disabled.	

Invalid statistics type value

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The only valid statistics types are individual and aggregate.	Enter a valid statistics type or ignore option.

Invalid unknown bandwidth type specified

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Two bandwidth types are supported: absolute and relative.	Enter a valid bandwidth type.

Invalid unsupported buffering capabilities value specified

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The buffering capabilities are not supported.	Check platform documentation and use a compatible buffering setting.

Invalid unsupported copy-to-cpu option specified

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The copy-to-CPU can have two values, true or false. It's possible that the only supported value for the target entry is false.	Check the documentation if necessary and use a valid copy-to-CPU option.

Comments? infodev@avaya.com

Invalid unsupported DAPP enable value specified

Type/ Severity	Source	Description	Remedial Action
Serious	QoS	DAAP can be enabled with or without status.	Specify a valid enable value or disable DAAP.

Invalid unsupported DAPP maximum IPv4 ICMP length specified

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The maximum IPv4 ICMP length must be between 0 and 1023.	Enter a valid/supported length in that range.

Invalid unsupported DAPP maximum IPv6 ICMP length specified

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The maximum Ipv6 ICMP length must be between 0 and 16383.	Enter a valid/supported length in that range.

Invalid unsupported DAPP minimum TCP header length specified

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The minimum TCP header length must be within 0 to 255.	Enter a valid/supported length in the specified range.

Invalid unsupported default gateway address length specified

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The default gateway address length must be 4 (IPv4) and 16 (IPv6).	Specify a valid default gateway address length.

Invalid unsupported default gateway address specified

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The default gateway provided is not a valid interface application IP address.	Specify a valid IP default gateway address.

Invalid unsupported destination IP address length specified

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Destination address is too short/long.	Enter a proper address with length 4 (ipv4) or 16 (ipv6).

Invalid unsupported DHCP server address length specified

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The DHCP server address length must be 4 (IPv4) and 16 (IPv6).	Specify a valid DHCP server address length.

Comments? infodev@avaya.com

Invalid unsupported DHCP server address specified

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The DHCP address provided is not a valid interface application IP address.	Specify a valid IP DHCP server address.

Invalid unsupported interface type specified

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The valid interface types for the interface applications are access and core.	Enter one of the valid interface types.

Invalid unsupported mirror frame option specified

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The mirror frame option can have two values, true or false. It's possible that the only supported value for the target entry is false.	Check the documentation if necessary and use a valid mirror frame option.

Invalid unsupported NT application mode value specified

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The only supported AutoQoS modes are disabled, pure and mixed.	The only supported AutoQoS modes are disabled, pure and mixed.

Invalid unsupported packet type value specified

Type/ Severity	Source	Description	Remedial Action
Serious	QoS	Invalid value specified. Packet-types supported: etherII, llc, snap.	Specify a supported packet type.

Invalid unsupported QoS system operational mode value specified

Type/Severity	Source	Description	Remedial Action
Serious	QoS	If the current platforms supports QoS system disabled state then the operational mode can be either disabled or enabled. Otherwise the QoS system operational mode can only be enabled.	Specify a supported QoS operational mode regarding the current platform.

Invalid unsupported queue configuration value specified

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The queue set value must be between 1 and 8.	Specify a queue set value in the range described.

Invalid unsupported role assoc compatibility specified

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The supported role association are loose and strict.	Specify a supported/valid role association.

Comments? infodev@avaya.com

Invalid unsupported source IP address length specified

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Source address is too short/long.	Enter a proper address with length 4 (ipv4) or 16 (ipv6).

Invalid unsupported Trusted processing mode value specified

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Trusted processing modes can be partial or full. Any other modes are invalid or unsupported.	Specify a valid trusted processing mode.

Invalid unsupported UBP support level value specified

Type/Severity	Source	Description	Remedial Action
Serious	QoS	There are 4 user based policies levels supported, the first one being “disabled”.	Enter a valid user based policy support.

Invalid unsupported VLAN tag value specified (VLAN tag)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Invalid VLAN tag, it must be tagged, untagged or not specified (ignore).	Enter an appropriate VLAN tag (tagged, untagged or ignore).

Invalid update DSCP value specified (not currently supported)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The specified update DSCP value is currently not supported.	Check the documentation if necessary and use a supported update DSCP value.

Invalid update priority value specified

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The only valid update priorities values are between 0 and 7.	Enter a valid update priority value.

Invalid update VLAN Id specified (VLAN Id)

Type/ Severity	Source	Description	Remedial Action
Serious	QoS	The update VLAN Id must be between 1 and 4094.	Enter a valid update VLAN Id in that range.

Invalid user priority match selection specified (priority value)

Type/ Severity	Source	Description	Remedial Action
Serious	QoS	The user priority value must be between 0 and 7 or all.	Enter a valid user priority value.

Comments? infodev@avaya.com

IPv4-only filter criteria mixed with IPv6 criteria

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Ipv4 and IPv6 fields detected in the same filter.	Separate IPv4 and Ipv6 options in two filters.

IP classifier entry still referenced (deletion prohibited)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Cannot delete an ip classifier element if it's referenced in a classifier.	Remove the classifier first.

IP destination address and mask values out-of-sync

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The destination address and prefix do not correspond (at least one address bit not included in mask is set).	Modify the address or mask.

IP destination Layer 4 port maximum value out-of-range (dest port#

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The maximum IP protocol destination port value must be between 0 and 65535.	Enter a valid maximum IP protocol destination port in the range specified.

IP destination Layer 4 port minimum value out-of-range (dest port#)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The minimum IP protocol destination port value must be between 0 and 65535.	Enter a valid minimum IP protocol destination port in the range specified.

IP protocol value out-of-range (IP protocol#)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The IP protocol must be between 0 and 255.	Enter a valid IP protocol value.

IP source address and mask values out-of-sync

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The source address and prefix do not correspond (at least one bit not included in mask is set).	Modify the address or mask.

IP source Layer 4 port minimum value out-of-range (src port#)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The minimum IP protocol source port value must be between 0 and 65535.	Enter a valid minimum IP protocol source port in the range specified.

Comments? infodev@avaya.com

IP source Layer 4 port minimum value out-of-range (src port#)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The minimum IP protocol source port value must be between 0 and 65535.	Enter a valid minimum IP protocol source port in the range specified.

Issue detected enabling/disabling DSCP Mapping Table usage (port %d)

Parameters	Type/Severity	Source	Description	Remedial Action
Port number	Serious	QoS Agent	Unable to enable/disable usage of the DSCP Mapping table.	Reset device and retry.

Issue detected setting native DSCP Mapping Table values

Type/Severity	Source	Description	Remedial Action
Serious	QoS Agent	Unable to update settings in the DSCP Mapping table.	Reset device and retry.

Issue with classifier component mask detected

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Unable to create the classifier data mask structure form the classifier data provided.	Identify and separate the conflicting elements into multiple classifier blocks.

Layer 2 classifier still referenced (deletion prohibited)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Cannot delete a classifier if it is referenced in a classifier-block or policy.	Remove the classifier-block/policy first.

Layer 4 port filtering with IPv6 requires UDP TCP Next Header

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Port filtering is supported only for TCP and UDP protocols.	Specify next header: 6 for TCP or 17 for UDP or drop port filtering usage.

Layer 4 port range could not be reduced sufficiently

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The port range could not be reduce sufficiently for it's installation to be supported.	Modify the port range.

Meter (from clfr block) usage in multiple policies prohibited

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The meter specified in classifier block is already used by a policy.	Specify a different meter/ classifier block, create a new one or remove the conflicting policy.

Comments? infodev@avaya.com

Meter (from policy) usage in multiple policies prohibited

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The meter specified is already used by a policy.	Specify a different meter, create a new one or remove the conflicting policy.

Meter entry referenced by clfr block (deletion prohibited)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Cannot delete a meter if it's referenced in a classifier block.	Remove the classifier block first.

Meter entry referenced by meter (deletion prohibited)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Cannot delete a meter if it's referenced by another.	Delete the other meter first.

Meter entry referenced by policy (deletion prohibited)

Type/ Severity	Source	Description	Remedial Action
Serious	QoS	Cannot delete a meter if it's referenced by a policy.	Remove the policy first.

Meter identifier out-of-range (meter id)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	If it is a user entry the meter identifier must be between 1 and 55000. For a system entry the range is 55001-65535.	Enter a valid meter identifier.

Metering not supported with DS L2 access control lists

Type/ Severity	Source	Description	Remedial Action
Serious	QoS	Metering is not supported for ACLs DS(IP) or L2.	Enter DS/L2 classifier element or drop metering option.

Mirroring (requested via action) not configured correctly

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The metering is not configured correctly.	Inspect and correct the necessary entries, check documentation if necessary.

Modification of action (non-match usage) prohibited

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The action can not be modified currently as it is associated with a policy and not an individual classifier.	Remove the policy or create a new action.

Comments? infodev@avaya.com

No resources available for classifier port range checking

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The resources required are not available on all the ports in the specified range.	Modify either the port range or the demanding resources.

Non-match action contains conflicting data

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Unable to install the specified non-match action, conflicting data detected.	Identify conflicts and separate them into different non-match actions.

Non-match action not available for use with filter sets

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The non-match action drop must be deferred for access assign type NSNA, user based policy and traffic profile.	Remove the non-match action option.

Non-match action support not available on certain interfaces

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Non-match actions can only be applied to certain interfaces.	Specify a compatible interface or drop the non-match action.

Non-QoS interfaces may not be assigned to a role combination

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Interface type is prohibited. For example cascade (internal) ports should not be associated with a roleCombination since classification is prohibited on these interfaces.	Enter an interface compatible with QoS.

Non-supported action option (green action) specified

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Action criteria or storage type is not compatible with the action criteria type specified (green action).	Enter a compatible action.

Non-supported action option (in-profile action) specified

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Failed to validate the in-profile action that is associated. Certain actions may be required or forbidden.	Check documentation and use a valid in-profile action.

Non-supported action option (match action) specified

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Failed to validate the match action that is associated. Certain actions may be required or forbidden.	Check documentation and use a valid match action.

Comments? infodev@avaya.com

Non-supported action option (out-of-profile action) specified

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Failed to validate the out-of-profile action that is associated. Certain actions may be required or forbidden.	Check documentation and use a valid out-of-profile action.

Non-supported action option (policy non-match action) specified

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Failed to validate the non-match action that is associated. Certain actions may be required or forbidden.	Check documentation and use a valid non-match action.

Non-supported action option (red action) specified

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Action criteria or storage type is not compatible with the action criteria type specified (red action).	Enter a compatible action.

Non-supported action option (yellow action) specified

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Action criteria or storage type is not compatible with the action criteria type specified (yellow action).	Enter a compatible action.

NT application mode enable failure - inadequate resources

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The required resources for AutoQos to become enable are not available.	Check for and remove unneeded resources and try again.

Non-unique precedence order value detected (prohibited)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	There is already an existing mask on the specified precedence on the current interface.	Enter a different precedence/ interface or remove the conflicting mask.

Non-volatile QoS data discarded during restoration

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Certain QoS data was discarded (possible because of an upgrade).	Check the QoS data and complete it manually.

Non-volatile storage commit delay too large

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The maximum non-volatile storage commit delay is 604800.	Enter a smaller commit delay value.

Comments? infodev@avaya.com

Only one frame type supported per classifier

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The maximum frame types supported in a classifier is one.	Separate the frame types into multiple system classifiers.

Out-of-profile action contains conflicting data

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Unable to install the specified out-of-profile action, conflicting data detected.	Identify conflicts and separate them into different out-of-profile actions.

Out-of-range CoS index value (COS index value)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The valid CoS index range is 0 to 7.	Enter a CoS index value within the specified valid range.

Out-of-range queue index value (queue index) for in-use queue set

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The queue set must be between 1 and the runtime default queue set.	Check the agent default queue set and modify the value accordingly.

Out-of-range queue index value (queue index) for pending queue set

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The queue set must be between 1 and the runtime default queue set.	Check the agent default queue set and modify your value accordingly.

Packet redirection support limited by target interfaces

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Target interfaces are version 2 (Currently, all version 2 interfaces support redirection for all packet types or none) and do not support redirection for non-unicast packets.	Enter a different interface/port number.

Pattern matching data in excess of bytes# bytes specified

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The maximum pattern data length is 16 for 45XX and 32 for the rest of the platforms.	Separate the pattern matching data into multiple system classifiers so it fits the maximum length specified.

Pattern matching (Dst IP) not supported with IP addr type data

Type/Severity	Source	Description	Remedial Action
Serious	QoS	System classifiers with pattern matching (Dst IP) cannot be used with IP address type data.	Separate the conflicting elements into multiple classifier sets.

Comments? infodev@avaya.com

Pattern matching (Dst MAC) not supported with address type data

Type/Severity	Source	Description	Remedial Action
Serious	QoS	System classifiers with pattern matching (Dst MAC) cannot be used with address type data.	Separate the conflicting elements into multiple classifier sets.

Pattern matching (IP) not supported with non-IP addr type data

Type/Severity	Source	Description	Remedial Action
Serious	QoS	IP pattern matching (ipv4 or ipv6) used with UnknownNonIpMcast,NonIpMcast or NonIpPkt option.	Remove IP patter matching or non-IP type data from the system classifier.

Pattern matching not supported with other classification data

Type/Severity	Source	Description	Remedial Action
Serious	QoS	System classifiers with pattern matching can only be used with default ip or/and l2 classifiers in the same classifier set.	Separate the conflicting elements into multiple classifier sets.

Pattern modifier data specified without actual pattern data

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Pattern-related attributes have been set but pattern data is not specified.	Remove pattern-related attributes or specify patter data to avoid confusion.

Pattern position and data strings must be same length

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Different lengths detected: pattern position and data strings.	Use pattern position and data strings of the same length.

Policies with session data must be port-based

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Session policies must be port-based.	Modify the user policy entry or remove the session data.

Policy action out-of-range (action#)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	If this is a user policy the action id must be between 1 and 55000. For a system entry the range is 55001-65535.	Specify a valid action id.

Policy content incompatible with target interface(s)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The classifier(s) filter options used in the policy are not compatible with the target interface.	Enter a different interface or adapt classifier/policy.

Comments? infodev@avaya.com

Policy mask availability issue (space exhausted)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Unable to find next available mask precedence for the specified port.	Check for and remove unneeded resources on that port.

Policy modification support limited

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Policies under system control can be deleted but not modified. For user policies only certain modification are supported (if-group, port, name).	To change a different option remove policy and create a new one.

Policy non-match action out-of-range (non-match action#)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	If this is a user policy the non-match action id must be between 1 and 55000. For a system entry the range is 55001-65535.	Specify a valid non-match action id.

Policy precedence value out-of-range for target interface(s)

Type/ Severity	Source	Description	Remedial Action
Serious	QoS	Precedence limits differ based on the underlying hardware support.	Enter a precedence compatible with the hardware limits for the specified interface or use a different one.

Policy requirements exceed available resources (slot slot#)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Not all the resources required for the policy are available on the base or non-base unit(s).	Modify either the interfaces or the demanding resources.

Policy statistics index out-of-range (stats index)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Invalid policy tracking statistics. The supported types are: individual aggregate or disabled.	Specify a supported policy tracking statistics.

Policy precedence conflict detected with non-QoS application

Type/Severity	Source	Description	Remedial Action
Serious	QoS	A non-QoS application is already using the precedence specified.	Enter a different precedence.

Policy with this filtering values is already installed on this precedence

Type/Severity	Source	Description	Remedial Action
Serious	QoS	An identical policy detected on the same precedence and port.	Enter the existing policy.

Comments? infodev@avaya.com

Post-join ACL installation issue detected (ifc ifc#)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	ACL installation failed after a join stack event.	Try again or check the stack health. Further conclusions are drawn as this message appears either on base, non-base, all or some units in stack.

Post-join filter set installation issue detected (ifc ifc#)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Filter set installation failed after a join stack event.	Try again or check the stack health. Further conclusions are drawn as this message appears either on base, non-base, all or some of the units in stack.

Post-join traffic-profile installation issue detected (ifc ifc#)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Traffic-profile installation failed after a join stack event.	Try again or check the stack health. Further conclusions are drawn as this message appears either on base, non-base, all or some of the units in stack.

Potential inconsistent access asgn state (Undo fail) detected

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Inconsistent access assign state detected on the non base unit.	Try again later, reset the QoS agent, reset the unit or check the stack health.

Potential inconsistent ifc assignment state (Undo fail) detected

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Inconsistent interface assignment state detected on non base unit.	Try again later, reset the QoS agent or reset the unit.

Potential inconsistent policy state (Undo fail) detected

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Inconsistent policy state detected on non base unit.	Try again later, reset the QoS agent or reset the unit.

Precedence value out-of-range

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Precedence range depends on the platform.	Check documentation and use a valid precedence.

Comments? infodev@avaya.com

Provided metering information incomplete

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Insufficient or invalid information provided.	Specify a valid meter.

QoS policies may not be applied to uplink or daisy chain ports (port#)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	ESU Policies cannot be applied on daisy chain ports.	Enter different ports.

Queue configuration inconsistency detected (local queue conf stack queue conf)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The queue set is not same on all units in stack.	Try again later, reset the QoS agent or reset the unit.

Queue set assignment distribution across stack failed

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Unable to make changes across the stack.	Try later or check stack health.

Queue set unacceptable - pending range excludes in-use queues

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Cannot configure as a default queue set one that is currently used by a traffic shaping.	Enter an available queue set.

Queue set value modification prohibited

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The queue set may not be modified since the queue set association is created when the queue set is defined.	Verify that the queue set being specified is indeed the original queue set.

Rate granularity limited to increments of 1 Mbps or 64 Kbps

Type/Severity	Source	Description	Remedial Action
Serious	QoS	There are only two rate granularities supported: 1 Mbps and 64 Kbps.	Enter a rate with one of the supported granularities.

Rate (min) granularity limited (increments of 1 Mbps or 64 Kbps)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	There are only two rate granularities supported: 1 Mbps and 64 Kbps.	Enter a rate with one of the supported granularities.

Comments? infodev@avaya.com

Referenced block (by policy) deletion prohibited

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Cannot delete a classifier-block if it's referenced in a policy.	Remove the policy first.

Referenced set (by block) modifications prohibited

Type/Severity	Source	Description	Remedial Action
Serious	QoS	No modifications can be made to a classifier set referenced in a classifier-block.	Remove block, perform modifications and recreate classifier-block.

Referenced set (by policy) modifications prohibited

Type/Severity	Source	Description	Remedial Action
Serious	QoS	No modifications can be made to a classifier set used by a policy.	Remove policy, perform modifications and recreate policy.

Remote QoS-disable request failure (port# on unit unit#)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Failed to disable the Policy/ Interface.	Check for the conflicting entries, try again later, reset the QoS agent, reset the unit or check the stack health.

Request invalid - QoS interface apps enabled on interface(s)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Request is denied as the interface applications are enabled on this port.	Enter a different interface or disable the interface application on this port.

Request invalid - specified interface currently QoS-disabled

Type/Severity	Source	Description	Remedial Action
Serious	QoS	All request are denied when the target interface is QoS disabled.	Enter a different interface index.

Request temporarily denied - QoS support is currently disabled

Type/Severity	Source	Description	Remedial Action
Serious	QoS	All request are denied when QoS overall is disabled.	Enable QoS overall before committing any request.

Requested attribute usage is currently not supported

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The requested attribute is not compatible – attribute value support is limited.	Eliminate option or use a different attribute.

Comments? infodev@avaya.com

Requested filter manager support unavailable

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The requested operation is nor supported on the current hardware.	Change/drop the request.

Requested reserve data invalid

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Trying to remove an entry that is not actually reserved.	Check if the specified entry wasn't already removed.

Required bandwidth information not specified

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The queue bandwidth parameter has not been provided.	Specify the queue bandwidth parameter based on the bandwidth allocation attribute.

Resources exhausted (maximum class entries reached)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The maximum entries allowed for the class you are trying to configure an entry has been reached.	Check for and remove the related QoS entries that are not needed.

Resources exhausted (out-of-memory)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Memory allocation for the new entry failed.	Check for and remove the QoS entries that are not needed.

Role combination associated with interface (deletion prohibited)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Cannot remove a role combination if it's associated with an interface.	Associate a different interface role combination to the interface before requesting the removal.

Role combination contains unacceptable characters

Type/Severity	Source	Description	Remedial Action
Serious	QoS	A valid role combination contains letters, digits, special characters (period, line, plus, underline but not on the first position) and '$' but only as the first character.	Enter valid characters for the access element's label.

Role combination referenced by policy (deletion prohibited)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Cannot remove a role combination if it's referenced by a policy.	Remove the policy first.

Comments? infodev@avaya.com

Role (interface) capabilities incompatible with policy data

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The policy and the specified role(the component interfaces) have different version capabilities.	Enter either a role with compatible interface(s) or adapt the policy to match the required version.

Source MAC address and mask values out-of-sync

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The source MAC address and mask do not correspond (at least one address bit not included in mask is set).	Modify the source MAC address or mask.

Specified filter criteria is invalid inconsistent

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Invalid/inconsistent filter criteria detected in classifier.	Identify and remove the inconsistent/invalid data.

Specified policy components (classifiers) conflicting

Type/Severity	Source	Description	Remedial Action
Serious	QoS	All the masks/filters must correspond.	Separate conflicting classifiers into multiple policies.

Specified queue set information invalid

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Invalid information regarding queue set (queue number must be in supported range and the egress flag must be set).	Correct queue information and try again.

Specified token bucket criteria out of range

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Unsupported meter rate range specified.	Enter a supported meter rate range.

Src Layer 4 port min max values invalid (max must be = to min)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The maximum source port must be bigger than the minimum destination port.	Correct source port range limits.

srTCM meter issue - CIR must be the same in both meters

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Different CIRs detected in the two meters.	Enter the same CIR for both meters.

Comments? infodev@avaya.com

srTCM meter issue - EBS must be greater than CBS

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The burst size is not consistent.	Enter a EBS that is greater than CBS.

srTCM trTCM meter issue - diff algorithms in associated meters

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Meter types and rate values are not synchronized .	Associate a single algorithm for a meter.

srTCM trTCM meter issue - referenced meter incompatible unknown

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The referenced meter is compatible (srTCM/trTCM issue).	Check for and remove any conflicts or incompatible data.

srTCM trTCM meter issue - too many cascaded meters

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Meter cascade level is limited to two.	Enter only two meter cascade levels.

Specified Destination Layer 4 min max range not supported

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The destination port range is not supported.	Check the documentation if necessary and adapt it to a supported port range.

Specified inner VLAN ID min max range not supported

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Inner VLAN ID range not supported.	Check the documentation if necessary and adapt it to a supported port range.

Specified metering operation not supported

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The metering operation is not supported on the target hardware.	Create and use a compatible meter.

Specified metering statistics entry already in-use (by policy)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Installing a meter with the same statistics entry already in use by a policy is not allowed, even though sharing a counter entry across meters is supported.	Enter a different statistics entry or remove the policy(s).

Comments? infodev@avaya.com

Specified policy components (classifiers) conflicting

Type/Severity	Source	Description	Remedial Action
Serious	QoS	All the masks/filters must correspond.	Separate conflicting classifiers into multiple policies.

Specified policy statistics entry already in-use (by meter)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The same statistics entry is already associated with a meter. This is currently not allowed. Sharing a count entry across policies is supported.	Enter a different statistics entry or remove the meter.

Specified Source Layer 4 min max range not supported

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The source port range is not supported.	Check the documentation if necessary and adapt it to a supported port range.

Specified token bucket refresh interval not supported

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The refresh interval must be 8.	Enter the correct refresh interval.

Specified token bucket size (burst size) not supported

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The only supported token bucket sizes are 2^n K where n must be between 2 and 14.	Enter one of the valid token bucket sizes.

Specified user policy interface currently QoS-disabled

Type/Severity	Source	Description	Remedial Action
Serious	QoS	You cannot configure a user policy entry if the target interface is QoS disabled.	Choose a different interface.

Specified VLAN ID min max range not supported

Type/Severity	Source	Description	Remedial Action
Serious	QoS	VLAN ID range not supported.	Check the documentation if necessary and adapt it to a supported port range.

System classifier still referenced (deletion prohibited)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Cannot delete a system classifier element if it's referenced in a classifier.	Remove the classifier first.

Comments? infodev@avaya.com

TCP Control Flag filter criteria requires TCP protocol

Type/Severity	Source	Description	Remedial Action
Serious	QoS	TCP Control Flag filter criteria must be used with TCP protocol filter criteria.	Add the TCP protocol option.

Token bucket algorithm identifier invalid

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Invalid token bucket algorithm identifier.	Specify a valid token bucket identifier.

Token bucket algorithm identifier unknown unsupported

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Scheduling algorithm not found.	Specify an existing and valid algorithm identifier.

Token bucket minimum rate outside limits (64 - 10230000 Kbps)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The minimum bucket rate must be in the range specified.	Enter a bucket rate bigger than 64Kbps and smaller than 10230000 Kbps.

Token bucket entry referenced by meter (deletion prohibited)

Type/ Severity	Source	Description	Remedial Action
Serious	QoS	Cannot delete a token bucket entry if it's referenced in a meter.	Remove the meter first.

Token bucket entry referenced by shaper (deletion prohibited)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Cannot delete a token bucket if it's referenced in a shaper.	Remove shaper first.

Token bucket rate outside limits (64 - 10230000 Kbps)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The token bucket rate must be between 0 and 32Gbps.	Enter a rate value within that range.

Token bucket size not compatible with committed fill rate

Type/Severity	Source	Description	Remedial Action
Serious	QoS	For cos/queue shaping only MinRate and Rate are set so BurstSize must be >= Rate only when MinRate = 0.	Enter a valid token bucket size.

Comments? infodev@avaya.com

trTCM meter issue - PBS must be greater than CBS

Type/Severity	Source	Description	Remedial Action
Serious	QoS	PBS is not grater that CBS.	Modify options so that PIR is grater than CIR.

trTCM meter issue - PIR must be greater than CIR

Type/Severity	Source	Description	Remedial Action
Serious	QoS	PIR is not greater than CIR .	Modify options so that PIR is grater than CIR.

Traffic Prof filter set elem count exceeds available resources

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Although the element count is within the documented limit, the actual resources necessary may not be available due to the runtime configuration.	Check for and remove the resources that are not needed.

Traffic Prof filter set policy count (policy count) exceeds limit (policy limit)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The traffic profile filter set policy limit depends on the target hardware platform.	Check the documentation for the maximum number of traffic profile filter set policies allowed.

Traffic Prof filter set rule count (rule count) exceeds limit (rule limit)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The maximum number of rules for a traffic profile filter set is 75.	Separate the excess into multiple traffic profile filter sets.

Trusted processing mode change rejected - inadequate resources

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Unable to commit trusted processing mode transition form partial to full. Not enough resources available.	Check for and remove unneeded resources.

Unable to add block member (block elem# component set id) to existing policy

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Failed to install the specified classifier-block.	Check for available resources, interface capabilities or possible conflicts.

Unable to apply existing policy data to interface (unit# port#)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The interface assignment change needs to add the port to an existing policy.	Check the available/not needed resources.

Comments? infodev@avaya.com

Unable to apply existing user-based policy data to new user

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The system failed to clone the policy and the meter data that is associated with the current user.	Check log for related details on the issue. Try again later, reset the QoS agent, or reset the stack

Unable to apply filter set to ports (unsupported capabilities)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The filter set cannot be applied to the specified ports as the required interface capabilities are not compatible with all the interfaces.	Check the interface capabilities, and adapt the port mask for the operation to succeed.

Unable to apply newly-defined UBP filter set to existing user

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The system failed to apply the defined user based policy filter set to the existing user.	Check log for related details on the issue. Try again later, reset the QoS agent, or reset the stack.

Unable to apply pre-defined UBP filter set to new user

Type/ Severity	Source	Description	Remedial Action
Serious	QoS	Unable to install/update a UBP filter set for a new user.	Free resources/update UBP filter set

Unable to compress classification criteria in set adequately

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Failed to compress the combination of classification data elements from the individual classifiers.	Separate the conflicting elements into multiple classifier sets.

Unable to create out-of-profile action for access assignment

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Failed to create out-of-profile action for access assignment on base or non-base unit.	Check the log for the related details on the issue. Try again later, reset the QoS agent or reset the stack.

Unable to create count action (meter) for access assignment

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Failed to count action (from meter) for access assignment on base or non-base unit (if the stack is preset).	Check log for the related details on the issue. Try again later, reset the QoS agent or reset the stack.

Unable to create count action (policy) for access assignment

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Failed to count action (from policy) for access assignment on base or non-base unit.	Check log for related details on the issue. Try again later, reset the QoS agent, or reset the stack.

Comments? infodev@avaya.com

Unable to create count action (secondary meter) for access asgn

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Failed to create the count action component for ACL.	Check log for related details on the issue. Try again later, reset the QoS agent, or reset the stack.

Unable to create metering data for access assignment

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Failed to create metering data for access assignment on base or non-base unit.	Check log for the related details on the issue. Try again later, reset the QoS agent or reset the stack.

Unable to create non-match components for ACL

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Failed to create a non-match action component for ACL.	Check log for related details on the issue. Try again later, reset the QoS agent, or reset the stack.

Unable to create token bucket data for access assignment

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Failed to create the token bucket data for the access assignment on base or non-base unit.	Check log for the related details on the issue. Try again later, reset the QoS agent or reset the stack.

Unable to create policy data for access assignment

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Failed to create policy data for access assignment on base or non-base unit.	Check log for related details on the issue. Try again later, reset the QoS agent, or reset the stack.

Unable to create secondary metering data for access assignment

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Failed to create secondary metering data for ACL.	Check log for related details on the issue. Try again later, reset the QoS agent, or reset the stack.

Unable to create secondary token bucket data for access asgn

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The system failed to create a secondary token bucket component for ACL.	Check log for related details on the issue. Try again later, reset the QoS agent, or reset the stack.

Unable to create yellow action for access assignment

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Failed to create yellow action component for ACL.	Check log for related details on the issue. Try again later, reset the QoS agent, or reset the stack.

Comments? infodev@avaya.com

Unable to deactivate policy associated with interface

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The resource policy deallocation failed.	Try again later, reset the QoS agent or reset the unit.

Unable to delete block member (block element# component set id) from existing policy

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Failed to remove the specified classifier-block .	Check for existing references, possible conflicts or try again later.

Unable to delete UBP filter set on interface ifc#

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Failed to remove the user based policy filter set on the specified interface.	Check log for related details on the issue. Try again later, reset the QoS agent, or reset the stack.

Unable to derive suitable filter set element eval precedence

Type/Severity	Source	Description	Remedial Action
Serious	QoS	A precedence must be assigned to a filter set; else it cannot be installed on the interface.	Check the available un-needed resources, try again later, reset the QoS agent or reset the unit.

Unable to determine clfr interface(s) compatibility

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Unable to make changes because the system failed to determine classifier/ interface(s) compatibility version.	Enter a different classifier/ interface, try again later, reset the QoS agent or reset the unit.

Unable to disable ARP Spoofing support on interface (ifc#)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The system failed to disable the ARP Spoofing support on the specified interface.	Check log for related details on the issue. Try again later, reset the QoS agent, or reset the stack.

Unable to disable BPDUBlkr support on interface (ifc#)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Failed to disable BPDUBlkr policy data on the specified interface.	Check log for related details on the issue. Try again later, reset the QoS agent or reset the stack.

Unable to disable DHCP Snooping support on interface (ifc#)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The system failed to disable the DHCP Snooping support on the specified interface.	Check log for related details on the issue. Try again later, reset the QoS agent or reset the stack.

Comments? infodev@avaya.com

Unable to disable DHCP Spoofing support on interface (ifc#)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The system failed to disable the DHCP Spoofing support on the specified interface.	Check log for related details on the issue. Try again later, reset the QoS agent, or reset the stack.

Unable to disable DNSPort support on interface (ifc#)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The system failed to disable the DNSPort policy data on the specified interface.	Check log for related details on the issue. Try again later, reset the QoS agent, or reset the stack.

Unable to disable existing policy data on interface (unit# port#)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The interface assignment change needs to remove the port form an existing policy. This operation failed.	Check for and remove any conflicts regarding the interface.

Unable to disable FTPPort support on interface (ifc#)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The system failed to disable the FTPPort policy data on the specified interface.	Check log for related details on the issue. Try again later, reset the QoS agent, or reset the stack.

Unable to disable Nachia support on interface (ifc#)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The system failed to disable the Nachia policy data on the specified interface.	Check log for related details on the issue. Try again later, reset the QoS agent, or reset the stack.

Unable to disable policy data for access assignment

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Failed to disable the policy data.	Check log for related details on the issue. Try again later, reset the QoS agent, or reset the stack.

Unable to disable SQLSlam support on interface (ifc#)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The system failed to disable the SQLSlam policy data on the specified interface.	Check log for related details on the issue. Try again later, reset the QoS agent, or reset the stack.

Unable to disable SynFinScan support on interface (ifc#)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The system failed to disable the SynFinScan policy data on the specified interface.	Check log for related details on the issue. Try again later, reset the QoS agent, or reset the stack.

Comments? infodev@avaya.com

Unable to disable Xmas support on interface (ifc#)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The system failed to disable the Xmas policy data on the specified interface.	Check log for related details on the issue. Try again later, reset the QoS agent, or reset the stack.

Unable to enable ARP Spoofing support on interface (ifc#)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The system failed to enable the ARP Spoofing support on the specified interface.	Check log for related details on the issue. Try again later, reset the QoS agent, reset the stack, or use a different interface.

Unable to enable BPDUBlkr support on interface (ifc#)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The system failed to enable the BPDUBlkr policy data on the specified interface.	Check log for related details on the issue. Try again later, reset the QoS agent, reset the stack, or use a different interface.

Unable to enable DHCP Snooping support on interface (ifc#)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The system failed to enable the DHCP Snooping support on the specified interface.	Check log for related details on the issue. Try again later, reset the QoS agent, reset the stack, or use a different interface.

Unable to enable DHCP Spoofing support on interface (ifc#)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The system failed to enable the DHCP Spoofing support on the specified interface.	Check log for related details on the issue. Try again later, reset the QoS agent, reset the stack, or use a different interface.

Unable to enable DNSPort support on interface (ifc#)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The system failed to enable the DNSPort policy data on the specified interface.	Check log for related details on the issue. Try again later, reset the QoS agent, reset the stack, or use a different interface.

Unable to enable FTPPort support on interface (ifc#)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The system failed to enable the FTPPort policy data on the specified interface.	Check log for related details on the issue. Try again later, reset the QoS agent, reset the stack, or use a different interface.

Unable to enable Nachia support on interface (ifc#)

Type/ Severity	Source	Description	Remedial Action
Serious	QoS	The system failed to enable the Nachia policy data on the specified interface.	Check log for related details on the issue. Try again later, reset the QoS agent, reset the stack, or use a different interface.

Comments? infodev@avaya.com

Unable to enable policy data for access assignment

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Failed to enable the policy data.	Check log for related details on the issue. Try again later, reset the QoS agent, or reset the stack.

Unable to enable SQLSlam support on interface (ifc#)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The system failed to enable the SQLSlam policy data on the specified interface.	Check log for related details on the issue. Try again later, reset the QoS agent, reset the stack, or use a different interface.

Unable to enable SynFinScan support on interface (ifc#)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The system failed to enable the SynFinScan policy data on the specified interface.	Check log for related details on the issue. Try again later, reset the QoS agent, reset the stack, or use a different interface.

Unable to enable Xmas support on interface (ifc#)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The system failed to enable the Xmas policy data on the specified interface.	Check log for related details on the issue. Try again later, reset the QoS agent, reset the stack, or use a different interface.

Unable to install access assignment - component creation issue

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Unable to create many of the access assignment components like: base action, token bucket entry, count action, meter, policy.	Check for the available or not needed resources.

Unable to manipulate DAPP support (no applicable interfaces)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The target interfaces data does not exist.	Enter an existing interface data.

Unable to modify access assignment - component modify issue

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Unable to make changes as one of the modifications required for an access assignment component failed.	Check the log for a more detailed information on the issue. Try again later, reset the QoS agent, or reset the stack.

Unicast (Interface#) and Non-Unicast (interface#) interfaces in conflict

Type/ Severity	Source	Description	Remedial Action
Serious	QoS	The interface number for unicat and non-unicast does not correspond.	Enter the same interface/port number.

Comments? infodev@avaya.com

Unknown incompatible access element specified

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The access element specified does not exist or the storage type is not compatible.	Specify a compatible access element.

Unknown incompatible action component specified

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Specified action doesn't exists or it's system/agent entry.	Enter an existing action or create a new one.

Unknown incompatible classifier block specified

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The classifier block does not exist.	Enter an existing classifier block or create a new one.

Unknown incompatible classifier set specified

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The specified classifier set does not exist.	Enter an existing classifier set or create a new one.

Unknown incompatible in-profile action specified

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The in-profile action specified is unknown or incompatible.	Check log for other possible details on the issue. Verify that the in-profile action exists and is compatible with the entry.

Unknown incompatible in-profile (green) action specified

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Action criteria or storage type is not compatible with the action criteria type specified (in-profile green).	Enter a compatible in-profile action.

Unknown incompatible match action specified

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The specified action does not exist.	Enter an existing action or create a new one.

Unknown incompatible metering component specified

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The metering component is unknown or not compatible.	Verify that the metering component exists and also that the storage types of the entries are compatible.

Comments? infodev@avaya.com

Unknown incompatible metering statistics entry specified

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Unknown or incompatible statistics with policy storage type.	Enter different statistics type.

Unknown incompatible out-of-profile action specified

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The out-of-profile action specified is unknown or incompatible.	Check log for other possible details on the issue. Verify that the out-of-profile action exists and is compatible with the entry.

Unknown incompatible out-of-profile (red) action specified

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Action criteria or storage type is not compatible with the action criteria type specified (out-of-profile red).	Enter a compatible out-of-profile action.

Unknown incompatible out-of-profile (yellow) action specified

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Action criteria or storage type is not compatible with the action criteria type specified (out-of-profile yellow).	Enter a compatible out-of-profile action.

Unknown incompatible policy statistics entry specified

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Unknown or incompatible statistics with policy storage type.	Enter different statistics type.

Unknown incompatible policy non-match action specified

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The specified non-match action does not exist.	Enter an existing non-match action or create a new one.

Unknown incompatible queue set specified

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The queue set specified is unknown.	Use an existing queue set.

Unknown incompatible role combination specified

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Referenced role must exist/be stable prior to entry creation/modification.	Make sure the role combination exists or create a new one.

Comments? infodev@avaya.com

Unknown incompatible token bucket reference specified

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The token bucket specified is not valid.	Check the documentation and use a valid token bucket.

Unknown out-of-range interface index value (ifc#)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The interface index does not exist.	Check the platform's/stack's port range and use a valid interface index.

Unknown out-of-range interface index value (ifc index)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The interface index does not exist.	Check the port range of the platform or the stack, and use a valid interface index.

Unknown unsupported StorageType specified

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The supported storage types are: volatile, non-volatile, permanent, read-only and other. Also, take into account that certain actions/entries require certain storage types.	Check the documentation if necessary and use a compatible/valid storage type.

Unknown unsupported interface application type specified

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The interface application type provided is unknown or unsupported.	Check documentation and use a valid interface application type.

Unknown unsupported interface class specified (ifc class)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The valid interface classes are trusted, untrusted and unrestricted.	Enter a valid/supported interface class.

Unknown unsupported IP Flag specified

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The specified IP Flag is not supported.	Check documentation if necessary and enter a valid IP Flag.

Unknown unsupported TCP Control Flag specified

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The specified TCP Control Flag is not supported.	Check documentation if necessary and enter a valid TCP Control Flag.

Comments? infodev@avaya.com

Unknown queue set queue reference detected

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The specified queue (set) does not exist.	Enter an existing queue/ queue set.

Unsupported IP address type specified

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Unsupported address type provided. (It should not get here) Internal error.	Enter a ipv4 or ipv6 address.

Unsupported pattern offset data specified

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Position data and pattern data cannot be processed correctly into an appropriate mask.	Change or separate the pattern data into multiple system classifiers.

Unsupported unknown QoS agent configuration attribute (attribute#)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The attribute you are trying to configure is not supported/recognized by the QoS agent.	Remove the attribute.

Update priority value and update DSCP value out-of-sync

Type/Severity	Source	Description	Remedial Action
Serious	QoS	If the priority update is set to be done based on DSCP-to-user priority map (egressmap) the DSCP value must be specified.	Change the update priority type or specify a DSCP value.

Update priority value per ingress DSCP currently not supported

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Priority update based on 802.1p priority-to-DSCP map (ingressmap) is not currently supported.	Change the update priority type.

User Policy (UBP) filter set in use (QoS disable prohibited)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Cannot disable the QoS system if there still are user policies in use.	Remove the user policies first.

User Policy (UBP) filter set in use (QoS reset prohibited)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Cannot reset the QoS engine if the user policy filter sets are still in use.	Remove or disable the user policy filter sets before re-setting the QoS engine.

Comments? infodev@avaya.com

User Policy data referencing interface (operation prohibited)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	There are non-QoS applications that have created entries that reference this interface.	Remove all references before performing other operations.

User policy filter set count (<set count>) exceeds limit (<set limit>)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The user policy filter set limit depends on the target hardware platform.	Check documentation for the maximum number of user policy filter sets allowed.

User policy filter set element count exceeds available resources

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The policy filter set element count limit depends on the target hardware platform.	Check the documentation for the maximum number of policy filter set elements allowed.

User policy group contains invalid unacceptable characters

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Only printable characters are allowed.	Enter valid characters for the policy group.

User policy group length outside of acceptable limits

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The maximum user policy group length is 64.	Separate the entries into multiple policy groups.

User policy name contains invalid unacceptable characters

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Only printable characters are allowed.	Enter valid characters for the policy label.

User policy name length outside of acceptable limits

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The maximum length for a policy name is 64.	Enter a policy name within the specified limit.

User priority specified with untagged frames (invalid)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	User priority appears in tagged frames.	Drop either priority or untagged option.

VLAN ID min max values invalid (min VLAN ID ! max VLAN ID)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	Max VLAN ID value must be bigger that min value.	Correct the VLAN ID range limits.

Comments? infodev@avaya.com

VLAN range could not be reduced sufficiently

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The VLAN range could not be reduce sufficiently for it's installation to be supported.	Modify the VLAN range.

Incompatible in-profile action (untrustedv4v6 ifc)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The specified in-profile action is not compatible with the associated interface type (untrustedv4v6).	Enter a different in-profile action or change the interface group assignment.

Incompatible out-of-profile action (untrustedv4v6 ifc)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The specified out-of-profile action is not compatible with the associated interface type (untrustedv4v6).	Enter a different out-of-profile action or change the interface group assignment.

Unable to apply pre-defined UBP filter set to new user (port %d/%d)

Type/Severity	Source	Description	Remedial Action
Information	Serious	The agent failed to install the corresponding UBP filter.	Check the log for a previous more detailed message or the current available hardware resources.

Unable to inform SPB of ifc assignment change (%d/%d)

Type/Severity	Source	Description	Remedial Action
Critical	QoS	SPB might not be aware of the current QoS interface type class of the specified interface.	Force a transition on the specified interface.

Incompatible match action (untrustedv4v6 ifc)

Type/Severity	Source	Description	Remedial Action
Serious	QoS	The specified action is not compatible with the associated interface type (untrustedv4v6).	Enter a different action or change the interface group assignment.

QoS information messages

802.1p user priority value modification prohibited

Type/Severity	Source	Description	Remedial Action
Information	QoS	Since the COS-to-DSCP default assignment association is created at initialization, the CoS may not be modified.	Verify that the COS being specified is indeed the original COS.

Comments? infodev@avaya.com

Access assignment distribution across stack failed

Type/Severity	Source	Description	Remedial Action
Information	QoS	Unable to carry out the access assignment distribution across the stack.	Try later or check the stack health.

Access element distribution across stack failed

Type/Severity	Source	Description	Remedial Action
Information	QoS	Unable to access the element distribution across the stack.	Try later or check stack health.

Agent configuration distribution across stack failed

Type/Severity	Source	Description	Remedial Action
Information	QoS	Unable to commit changes across the stack.	Unable to commit changes across the stack.

Base action distribution across stack failed

Type/Severity	Source	Description	Remedial Action
Information	QoS	Unable to commit base action distribution across the stack.	Try later or check the stack health.

Capabilities determined by agent (not-writable)

Type/Severity	Source	Description	Remedial Action
Information	QoS	The interface type capabilities cannot be modified.	Eliminate option.

Classifier block distribution across stack failed

Type/Severity	Source	Description	Remedial Action
Information	QoS	Unable to commit changes across the stack.	Try later or check stack health.

Classifier component distribution across stack failed

Type/Severity	Source	Description	Remedial Action
Information	QoS	Unable to commit changes across the stack.	Try later or check stack health.

Conflicting egress interface and egress trunk data specified

Type/Severity	Source	Description	Remedial Action
Information	FCoE Redirect	FCoE Redirect profile element data is not correct.	Specify all required profile data.

Comments? infodev@avaya.com

COS mapping distribution across stack failed

Type/Severity	Source	Description	Remedial Action
Information	QoS	Unable to commit COS mapping distribution across the stack.	Try later or check stack health.

CoS shaping distribution across stack failed

Type/Severity	Source	Description	Remedial Action
Information	QoS	Unable to make CoS shaping distribution across the stack.	Try later or check the stack health.

Count action distribution across stack failed

Type/Severity	Source	Description	Remedial Action
Information	QoS	Unable to commit changes across the stack.	Try later or check stack health.

DAPP-detected DoS attack blocked unit unit# (many ports)

Type/Severity	Source	Description	Remedial Action
Information	QoS	A Denial of Service attack was blocked on the specified unit and on multiple ports.	No action required.

DAPP-detected DoS attack blocked unit unit# port port#

Type/Severity	Source	Description	Remedial Action
Information	QoS	A Denial of Service attack was blocked on the specified unit and port.	No action required.

DAPP support disable failure

Type/ Severity	Source	Description	Remedial Action
Information	QoS	Unable to commit changes (disable DAAP) across the stack.	Try again later, reset the QoS agent, reset the unit or check stack health.

DAPP support enable failure

Type/Severity	Source	Description	Remedial Action
Information	QoS	Unable to commit changes (enable DAAP) across the stack.	Try again later, reset the QoS agent, reset the unit or check stack health.

Data distribution class class# across stack failed

Type/Severity	Source	Description	Remedial Action
Information	QoS	Unable to commit changes across the stack.	Try later or check the stack health.

Comments? infodev@avaya.com

DSCP mapping distribution across stack failed

Type/Severity	Source	Description	Remedial Action
Information	QoS	Unable to commit DSCP mapping distribution across the stack.	Try later or check stack health.

DSCP value modification prohibited

Type/Severity	Source	Description	Remedial Action
Information	QoS	Since the qset/dscp-to-queue assignment association is created when the qset (queue set) is defined including the creation of an element per DSCP value, the DSCP may not be modified. Also, only IPv4/IPv6 packets can have the DSCP value updated.	Verify that the DSCP being specified is indeed the original DSCP or eliminate option if not an Ipv4/IPv6 packet.

Duplicate entry detected (prohibited)

Type/Severity	Source	Description	Remedial Action
Information	QoS	The QoS entry already exists.	Use the existing entry if possible.

Duplicate FCoE redirection entry detected

Type/Severity	Source	Description	Remedial Action
Information	QOS	Duplicate FCoE redirection entry detected.	No action required.

Egress interface or trunk data is required - data missing

Type/Severity	Source	Description	Remedial Action
Information	FCoE Redirect	FCoE Redirect profile element data is not complete.	Specify all required profile data.

Element deletion prohibited (permanent read-only system entry)

Type/Severity	Source	Description	Remedial Action
Information	QoS	" System-owned policies cannot be deleted via the normal commands. Some of them may be removed through certain “disable” commands. "	Check the documentation if necessary and use the appropriate disable command(s) where possible.

Element label not acceptable - reserved

Type/Severity	Source	Description	Remedial Action
Information	QoS	The label is reserved in the system.	Enter a different label.

Element may only be modified not created or deleted

Type/Severity	Source	Description	Remedial Action
Information	QoS	The specified element can only be modified. Possible entries: COS-to-DSCP assignment default values created at initialization; default DSCP-to-queue assignments and default CoS-to-queue assignments	Modify the existing entry if necessary.

Comments? infodev@avaya.com

Type/Severity	Source	Description	Remedial Action
		created when a new queue set is defined.	

Element modification prohibited (read-only or system entry)

Type/Severity	Source	Description	Remedial Action
Information	QoS	You cannot modify or remove a read-only or system entry.	Create a similar entry with the proper modifications if necessary.

FCoE controller ifIndex not set - FCoE redirection enable prohibited

Type/Severity	Source	Description	Remedial Action
Information	FCoE Redirect	Required FCoE controller data not defined.	Specify FCoE controller data.

FCoE controller VLAN not set - FCoE redirection enable prohibited

Type/Severity	Source	Description	Remedial Action
Information	FCoE Redirect	Required FCoE controller data not defined.	Specify FCoE controller data.

Index value out-of-range

Type/Severity	Source	Description	Remedial Action
Information	QoS	Invalid QoS entry index value. Either system index for a non-system entry, or index out of the supported range.	Enter a different entry index.

Invalid drop action option specifiedInvalid drop action option specified

Type/Severity	Source	Description	Remedial Action
Information	QoS	The valid/supported drop options are drop, don't drop and deferred. Take into account that for certain action types the deferred option is not valid.	Check the documentation if necessary and use a compatible/valid drop action option.

Invalid entry creation attempted (index index#)

Type/Severity	Source	Description	Remedial Action
Information	QoS	Creation of the specified QoS entry is not allowed (modifications may be supported) – possible entries: COS-to-DSCP assignment default values created at initialization; default DSCP-to-queue assignments and default CoS-to-queue assignments created when a new queue set is defined.	Modify the existing entry if necessary.

Invalid FCoE controller ingress interface specified

Type/Severity	Source	Description	Remedial Action
Information	FCoE Redirect	An invalid FCoE controller ingress interface was specified.	Specify a valid interface.

Comments? infodev@avaya.com

Invalid FCoE controller VLAN specified

Type/Severity	Source	Description	Remedial Action
Information	FCoE Redirect	An invalid FCoE controller VLAN was specified..	Specify a valid VLAN.

Invalid/unknown FCoE redirection egress trunk ID specified

Type/Severity	Source	Description	Remedial Action
Information	FCoE Redirect	An invalid FCoE redirection trunk ID was specified.	Specify a valid trunk ID.

Invalid update DSCP value specified (DSCP value)

Type/Severity	Source	Description	Remedial Action
Information	QoS	The valid DSCP values are between 0 and 63.	Enter a valid DSCP value (in the specified range).

Interface action distribution across stack failed

Type/Severity	Source	Description	Remedial Action
Information	QoS	Unable to perform action distribution changes across the stack.	Try later or check stack health.

Interface application distribution across stack failed

Type/Severity	Source	Description	Remedial Action
Information	QoS	Unable to carry out the interface application distribution across the stack.	Try later or check the stack health.

Interface assignment distribution across stack failed

Type/Severity	Source	Description	Remedial Action
Information	QoS	Unable to commit changes (interface assignment) across the stack.	Try later or check stack health.

IP classifier distribution across stack failed

Type/Severity	Source	Description	Remedial Action
Information	QoS	Unable to commit changes across the stack.	Try later or check stack health.

IP protocol value TCP or UDP needed with Layer 4 port filtering

Type/Severity	Source	Description	Remedial Action
Information	QoS	Port filtering can only be used with TCP or UDP protocols.	Specify the IP protocol to avoid any confusions.

Comments? infodev@avaya.com

Issue detected during QoS stack synchronization

Type/Severity	Source	Description	Remedial Action
Information	QoS	Delays are exhausted and the stack synchronization could not be verified.	Try later or check the stack health.

Issue detected enabling disabling DSCP table usage (port#)

Type/Severity	Source	Description	Remedial Action
Information	QoS	" Failed to set on the specified interface the port mode for usage of the global DSCP mapping table. "	Try again later, reset the QoS agent or reset the unit.

Issue detected setting native DSCP table values

Type/ Severity	Source	Description	Remedial Action
Information	QoS	Unable to set the native/ default DSCP table values.	Reset the QoS agent or reset the unit.

Layer 2 filter distribution across stack failed

Type/Severity	Source	Description	Remedial Action
Information	QoS	Unable to commit changes across the stack.	Try later or check stack health.

Lossless and Lossless-PFC modes are only supported in queue set 2

Type/Severity	Source	Description	Remedial Action
Information	QOS	Lossless and Lossless-PFC modes are only supported in queue set 2.	No action required.

Meter distribution across stack failed

Type/Severity	Source	Description	Remedial Action
Information	QoS	Unable to commit changes across the stack.	Try later or check stack health.

Network access settings for FCoE Redirect must be modified locally

Type/Severity	Source	Description	Remedial Action
Information	FCoE Redirect	Enable/disable of FCoE Redirect functionality limited to CLI.	Utilize CLI for feature enable/disable.

Non-unique element label detected (prohibited)

Type/Severity	Source	Description	Remedial Action
Information	QoS	The same label is used to identify a different entry of the same type.	Enter a different label.

Comments? infodev@avaya.com

Policy distribution across stack failed

Type/Severity	Source	Description	Remedial Action
Information	QoS	Unable to commit changes across the stack.	Try later or check stack health.

QoS inter-module communication issue detected

Type/Severity	Source	Description	Remedial Action
Information	QoS	Unable to make changes across the stack. If the request failed because of an RPC timeout, then this is due to a processing delay on the remote unit.	Check if a timeout issue, else try later or check the stack health.

Queue data distribution across stack failed

Type/Severity	Source	Description	Remedial Action
Information	QoS	Unable to commit queue data distribution across the stack.	Try later or check stack health.

Queue set value modification prohibited

Type/Severity	Source	Description	Remedial Action
Warning	QoS	The queue set may not be modified since the queue set association is created when the queue set is defined.	Verify that the queue set being specified is indeed the original queue set.

Queue shaping distribution across stack failed

Type/Severity	Source	Description	Remedial Action
Information	QoS	Unable to commit queue shaping distribution across the stack.	Try later or check the stack health.

Role combination length outside of acceptable limits

Type/ Severity	Source	Description	Remedial Action
Information	QoS	The maximum role combination length supported is 32.	Enter a valid role combination.

Role combination distribution across stack failed

Type/Severity	Source	Description	Remedial Action
Information	QoS	Unable to commit role combination distribution across the stack.	Try later or check stack health.

Simultaneous operations involving access asgn ifcs prohibited

Type/Severity	Source	Description	Remedial Action
Information	QoS	Other similar operations involving the specified access assignment/ interface(s) used by the policy are in progress.	Try again later after all the pending operations are completed.

Comments? infodev@avaya.com

Simultaneous operations involving policy blocks ifcs prohibited

Type/Severity	Source	Description	Remedial Action
Information	QoS	Other similar operations involving the interface used by the block/policy are in progress.	Try again later after all the pending operations are finished.

Simultaneous operations involving policies and blocks prohibited

Type/Severity	Source	Description	Remedial Action
Information	QoS	Other similar operations involving the specified block used by the policy are in progress.	Try again later after all the pending operations finished.

Simultaneous operations involving policies and ifcs prohibited

Type/Severity	Source	Description	Remedial Action
Information	QoS	Interfaces directly associated with a policy must be stable (active, not being created/deleted).	Try again later after all the pending operations finished.

System filter distribution across stack failed

Type/Severity	Source	Description	Remedial Action
Information	QoS	Unable to commit changes across the stack.	Try later or check stack health.

Token bucket data distribution across stack failed

Type/Severity	Source	Description	Remedial Action
Information	QoS	Unable to commit changes across the stack.	Try later or check stack health.

Traffic Prof filter set delete operation failed

Type/ Severity	Source	Description	Remedial Action
Information	QoS	Unable to carry out the delete operation on the traffic profile filter set across the stack.	Try later or check the stack health.

Traffic Prof filter set install operation failed

Type/Severity	Source	Description	Remedial Action
Information	QoS	Unable to carry out the installation on the traffic profile filter set across the stack.	Try later or check the stack health.

Traffic Prof filter set update operation failed

Type/Severity	Source	Description	Remedial Action
Information	QoS	Unable to carry out the update operation on the traffic profile filter set across the stack.	Try later or check the stack health.

Comments? infodev@avaya.com

Unable to inform SPB of ifc assignment change (%d/%d)

Parameters	Type/Severity	Source	Description	Remedial Action
Unit/Port	Information	QoS Agent	The information regarding an interface type class assigned to a port, failed to reach SPB.	If you are seeing this because of a QoS interface class modification and SPB is not used, the message can be ignored. Otherwise, a QoS class transition for the specified port forces the creation of a new message.

Unknown unsupported attribute specified (attribute)

Type/Severity	Source	Description	Remedial Action
Information	QoS	The specified attribute is not supported or unknown for the class you are trying to configure an entry	Check the documentation if necessary and use a supported attribute for that QoS class.

User policy distribution across stack failed

Type/Severity	Source	Description	Remedial Action
Information	QoS	Unable to commit user policy distribution across the stack.	Try later or check the stack health.

User policy filter set delete operation failed

Type/Severity	Source	Description	Remedial Action
Information	QoS	Unable to carry out the update operation on the policy filter set across the stack.	Try later or check the stack health.

User policy filter set install operation failed

Type/Severity	Source	Description	Remedial Action
Information	QoS	Unable to carry out the update operation on the policy filter set across the stack.	Try later or check the stack health.

User policy filter set update operation failed

Type/Severity	Source	Description	Remedial Action
Information	QoS	Unable to carry out the update operation on the policy filter set across the stack.	Try later or check the stack health.

Comments? infodev@avaya.com

Chapter 44: Quick Install messages

Quick Install information messages

QuickInstall console configuration error.

Type/Severity	Source	Description	Remedial Action
Information	Quick Install	Quick Install could not use the configuration from the console menu.	Use from console configuration or retry the menu with install command.

QuickInstall:console configuration success.

Type/Severity	Source	Description	Remedial Action
Information	Quick Install	Quick Install successfully executed the configuration from the console menu.	No action required.

QuickInstall: Error! Unable to locate agent software file

Type/Severity	Source	Description	Remedial Action
Information	QuickInstall	The agent file specified in “ ip.cfg” was not found.	Put agent file specified in “ip.cfg” file on USB device.

QuickInstall: Error! Unable to locate ASCII configuration file

Type/Severity	Source	Description	Remedial Action
Information	QuickInstall	The ASCII file specified in “ ip.cfg” was not found.	Put ASCII File specified in “ip.cfg” file on USB device.

QuickInstall: Error! Unable to locate diagnostics software file.

Type/Severity	Source	Description	Remedial Action
Information	QuickInstall	The diagnostic file specified in “ ip.cfg” was not found.	Put diagnostic file specified in “ip.cfg” file on USB device.

QuickInstall: Processing of USB config file has commenced.

Type/Severity	Source	Description	Remedial Action
Information	QuickInstall	USB file “ip.cfg” was found and script execution has commenced.	No action Required.

QuickInstall: Processing of USB config file is complete

Type/Severity	Source	Description	Remedial Action
Information	QuickInstall	The execution of script from “ip.cfg” is finished.	No action Required.

Comments? infodev@avaya.com

QuickInstall USB config file not found.

Type/Severity	Source	Description	Remedial Action
Information	Quick Install	Quick Install could not locate the USB file.	Put a file to USB script and set it to default if you want to run Quick Install.

QuickInstall USB file config error at line line#

Type/Severity	Source	Description	Remedial Action
Information	Quick Install	Quick Install detected an error in the script at the given line.	Correct the detected error at the specified line on the USB script and set it to default.

QuickInstall USB file config error - file exceed 200 lines.

Type/Severity	Source	Description	Remedial Action
Information	Quick Install	The script file is too large and exceeds the limit of 200 lines.	Remove some of the comments and the unnecessary lines.

QuickInstall USB file config error - file exceed 4096 bytes

Type/Severity	Source	Description	Remedial Action
Information	Quick Install	The script file is too large and exceeds the limit of 4096 bytes.	Remove some of the comments and the unnecessary lines.

QuickInstall:USB file config success.

Type/Severity	Source	Description	Remedial Action
Information	Quick Install	The script file from the USB is successfully executed by the Quick Install.	No action required.

Comments? infodev@avaya.com

Chapter 45: RADIUS Server Messages

Radius Server Messages

RADIUS authentication on stack serial disabled

Type/Severity	Source	Description	Remedial Action
Information	RADIUS	Informs user that RADIUS authentication was disabled on stack serial.	No action required.

RADIUS authentication on stack serial enabled

Type/Severity	Source	Description	Remedial Action
Information	RADIUS	Informs user that RADIUS authentication was enabled on stack serial.	No action required.

RADIUS authentication on stack telnet disabled

Type/Severity	Source	Description	Remedial Action
Information	RADIUS	Informs user that RADIUS authentication was	No action required.

Type/Severity	Source	Description	Remedial Action
		disabled on stack telnet.	

RADIUS authentication on stack telnet enabled

Type/Severity	Source	Description	Remedial Action
Information	RADIUS	Informs user that RADIUS authentication was enabled on stack telnet.	No action required.

RADIUS authentication on switch serial disabled

Type/Severity	Source	Description	Remedial Action
Information	RADIUS	Informs user that RADIUS authentication was disabled on switch serial.	No action required.

RADIUS authentication on switch serial enabled

Type/Severity	Source	Description	Remedial Action
Information	RADIUS	Informs user that RADIUS authentication was enabled on switch serial.	No action required.

Comments? infodev@avaya.com

RADIUS authentication on switch telnet disabled

Type/Severity	Source	Description	Remedial Action
Information	RADIUS	Informs user that RADIUS authentication was disabled on switch telnet.	No action required.

RADIUS authentication on switch telnet enabled

Type/Severity	Source	Description	Remedial Action
Information	RADIUS	Informs user that RADIUS authentication was enabled on switch telnet.	No action required.

Comments? infodev@avaya.com

Chapter 46: RADIUS Client messages

RADIUS Client information messages

Allowed connection attempt from user

Type/Severity	Source	Description	Remedial Action
Information	RADIUS Client	RADIUS: allowed connection attempt for the user starting with the given name.	No action required.

Disallowed connection Access Reject for user

Type/Severity	Source	Description	Remedial Action
Information	RADIUS Client	RADIUS - disallowed connection attempt for the user starting with the given name due to invalid user credentials.	Correct the user-configuration at the radius server; and retry entering valid user credentials.

Disallowed connection Invalid SvcType for user

Type/Severity	Source	Description	Remedial Action
Information	RADIUS Client	RADIUS - disallowed connection attempt for the user starting with the given name due to invalid service type	Send the correct svc-type from the radius server when needed.

RADIUS: ERROR - Couldn't create RADIUS Acct semaphore, errno %d

Type/Severity	Source	Description	Remedial Action
Information	Radius	The Radius Accounting task synchronization semaphore could not be created.	Reboot the stack.

RADIUS: ERROR - Couldn't create RADIUS semaphore, errno %d

Type/Severity	Source	Description	Remedial Action
Information	Radius	The Radius task synchronization semaphore could not be created.	Reboot the stack.

RADIUS: ERROR - Couldn't create RADIUS Acct semaphore, errno %d

Type/Severity	Source	Description	Remedial Action
Information	Radius	The Radius Accounting task synchronization semaphore could not be created.	Reboot the stack.

RADIUS: ERROR - Couldn't start RADIUS_client() task, errno %d

Type/Severity	Source	Description	Remedial Action
Information	Radius	The Radius client task could not start.	Reboot the stack.

Comments? infodev@avaya.com

RADIUS: ERROR - Couldn't start radius_recv() task, errno %d

Type/Severity	Source	Description	Remedial Action
Information	Radius	The Radius Receive task could not start.	Reboot the stack.

RADIUS: ERROR - Couldn't start RADIUS_AcctClient() task, errno %d

Type/Severity	Source	Description	Remedial Action
Information	Radius	The Radius Accounting task could not start.	Reboot the stack.

RADIUS: ERROR - Couldn't start RADIUS_ServerCheck() task, errno %d

Type/Severity	Source	Description	Remedial Action
Information	Radius	The Radius periodic reachability check task could not start.	Reboot the stack.

Comments? infodev@avaya.com

Chapter 47: Run Scripts messages

Run Scripts Information Messages

Error enabling IP Routing

Type/Severity	Source	Description	Remedial Action
Information	Run scripts: LLDP, ADAC	Cannot enable IP routing.	Check existing settings that could be in conflict with the script parameters. Undo settings or boot default the switch, then re-run the script, entering proper data input.

Error configuring 802.1AB

Type/Severity	Source	Description	Remedial Action
Information	Run scripts: IP Office, LLDP	Cannot configure LLDP med-network-policies or dot1q-framing tagging	Check existing settings that could be in conflict with the script parameters. Undo settings or boot default the switch, then re-run the script, entering proper data input.

Error configuring Management IP Address

Type/Severity	Source	Description	Remedial Action
Information	Run scripts:	IP address conflict	Check existing settings that could be in conflict with the

Type/Severity	Source	Description	Remedial Action
	LLDP, ADAC		script parameters. Undo settings or boot default the switch, then re-run the script, entering proper data input.

Error configuring port names

Type/Severity	Source	Description	Remedial Action
Information	Run scripts: IP Office	Cannot set port names.	Check existing settings that could be in conflict with the script parameters. Undo settings or boot default the switch, then re-run the script, entering proper data input.

Error configuring LLDP MED policies

Type/Severity	Source	Description	Remedial Action
Information	Run scripts: LLDP, ADAC	Cannot configure LLDP med-network-policies parameters.	Check existing settings that could be in conflict with the script parameters. Undo settings or boot default the switch, then re-run the script, entering proper data input.

Error creating Data VLAN

Type/Severity	Source	Description	Remedial Action
Information	Run scripts: IP Office, LLDP, ADAC	Cannot create new Data VLAN.	Check existing settings that could be in conflict with the script parameters. Undo settings or boot default the switch, then re-run the script, entering proper data input.

Comments? infodev@avaya.com

Error creating MLT

Type/Severity	Source	Description	Remedial Action
Information	Run scripts: ADAC	Cannot create new trunk for uplink ports.	Check existing settings that could be in conflict with the script parameters. Undo settings or boot default the switch, then re-run the script, entering proper data input.

Error creating Voice VLAN

Type/Severity	Source	Description	Remedial Action
Information	Run scripts: IP Office, LLDP, ADAC	Cannot create new Voice VLAN. (Maximum number of Voice Vlan reached)	Check existing settings that could be in conflict with the script parameters. Undo settings or boot default the switch, then re-run the script, entering proper data input.

Error deleting previously created cost 1 default route

Type/Severity	Source	Description	Remedial Action
Information	Run scripts: IP Office, LLDP, ADAC	Error delting default ip route.	Check existing settings that could be in conflict with the script parameters. Undo settings or boot default the switch, then re-run the script, entering proper data input.

Error deleting previously created Voice and Data VLANs

Type/Severity	Source	Description	Remedial Action
Information	Run scripts: IP Office, LLDP, ADAC	Error deleting existing VLAN.	Check existing settings that could be in conflict with the script parameters. Undo settings or boot default the switch, then re-run the script, entering proper data input.

Error enabling ADAC

Type/Severity	Source	Description	Remedial Action
Information	Run scripts: ADAC	Cannot enable ADAC.	Check existing settings that could be in conflict with the script parameters. Undo settings or boot default the switch, then re-run the script, entering proper data input.

Error enabling ADAC on ports

Type/Severity	Source	Description	Remedial Action
Information	Run scripts: ADAC	Cannot configure telephony ports.	Check existing settings that could be in conflict with the script parameters. Undo settings or boot default the switch, then re-run the script, entering proper data input.

Comments? infodev@avaya.com

Error enabling mstp learning on all ports

Type/Severity	Source	Description	Remedial Action
Information	Run scripts: IP Office	Cannot configure MSTP on ports.	Check existing settings that could be in conflict with the script parameters. Undo settings or boot default the switch, then re-run the script, entering proper data input.

Error enabling rstp learning on all ports

Type/Severity	Source	Description	Remedial Action
Information	Run scripts: IP Office	Cannot configure RSTP on ports.	Check existing settings that could be in conflict with the script parameters. Undo settings or boot default the switch, then re-run the script, entering proper data input.

Error executing script

Type/Severity	Source	Description	Remedial Action
Information	Run scripts: IP Office, LLDP, ADAC	Cannot continue with the script execution.	Check existing settings that could be in conflict with the script parameters. Undo settings or boot default the switch, then re-run the script, entering proper data input.

Error restoring management vlan to 1 or disabling ip routing

Type/Severity	Source	Description	Remedial Action
Information	Run scripts: IP Office, LLDP, ADAC	Previously configured settings (by user or another execution of the script) must be deleted at the beginning of the script to allow other settings to be made. In this case, IP routing cannot be disabled or the management vlan restored to VID 1.	Check existing settings that could be in conflict with the script parameters. Undo settings or boot default the switch, then re-run the script, entering proper data input.

Error saving configuration

Type/Severity	Source	Description	Remedial Action
Information	Run scripts: IP Office, LLDP, ADAC	Cannot save current configuration.	Check existing settings that could be in conflict with the script parameters. Undo settings or boot default the switch, then re-run the script, entering proper data input.

Error setting ADAC operating mode

Type/Severity	Source	Description	Remedial Action
Information	Run scripts: ADAC	Cannot set ADAC tagged frames operating mode.	Check existing settings that could be in conflict with the script parameters. Undo settings or boot default the switch, then re-run the script, entering proper data input.

Comments? infodev@avaya.com

Error setting call server ports

Type/Severity	Source	Description	Remedial Action
Information	Run scripts: ADAC	Cannot configure ports as Call-Server ports..	Check existing settings that could be in conflict with the script parameters. Undo settings or boot default the switch, then re-run the script, entering proper data input.

Error setting Data VLAN Gateway IP address and network mask

Type/Severity	Source	Description	Remedial Action
Information	Run scripts: IP Office, LLDP, ADAC	IP address conflict.	Check existing settings that could be in conflict with the script parameters. Undo settings or boot default the switch, then re-run the script, entering proper data input.

Error setting default IP Route

Type/Severity	Source	Description	Remedial Action
Information	Run scripts: IP Office, LLDP, ADAC	IP address conflict.	Check existing settings that could be in conflict with the script parameters. Undo settings or boot default the switch, then re-run the script, entering proper data input.

Error setting IP Office Call-Server IP address

Type/Severity	Source	Description	Remedial Action
Information	Run scripts: IP Office, LLDP, ADAC	Cannot configure Call-Server IP Address.	Check existing settings that could be in conflict with the script parameters. Undo settings or boot default the switch, then re-run the script, entering proper data input.

Error setting IP Office File-Server IP address

Type/Severity	Source	Description	Remedial Action
Information	Run scripts: IP Office, LLDP, ADAC	Cannot configure File-Server IP Address.	Check existing settings that could be in conflict with the script parameters. Undo settings or boot default the switch, then re-run the script, entering proper data input.

Error setting Management VLAN

Type/Severity	Source	Description	Remedial Action
Information	Run scripts: LLDP, ADAC	Cannot set Data V:AM as Management VLAN.	Check existing settings that could be in conflict with the script parameters. Undo settings or boot default the switch, then re-run the script, entering proper data input.

Comments? infodev@avaya.com

Error setting poe-priority high on ports

Type/Severity	Source	Description	Remedial Action
Information	Run scripts: IP Office	Cannot configure poe priority	Check existing settings that could be in conflict with the script parameters. Undo settings or boot default the switch, then re-run the script, entering proper data input.

Error setting QoS

Type/Severity	Source	Description	Remedial Action
Information	Run scripts: IP Office, LLDP	Cannot add new QoS interface group of trusted.	Check existing settings that could be in conflict with the script parameters. Undo settings or boot default the switch, then re-run the script, entering proper data input.

Error setting spanning-tree learning to fast on all ports

Type/Severity	Source	Description	Remedial Action
Information	Run scripts: IP Office, LLDP, ADAC	Cannot configure STP on ports.	Check existing settings that could be in conflict with the script parameters. Undo settings or boot default the switch, then re-run the script, entering proper data input.

Error setting uplink ports

Type/Severity	Source	Description	Remedial Action
Information	Run scripts:LLDP, ADAC	Cannot configure ports as Uplinks.	Check existing settings that could be in conflict with the script parameters. Undo settings or boot default the switch, then re-run the script, entering proper data input.

Error setting VLAN attributes

Type/Severity	Source	Description	Remedial Action
Information	Run scripts: IP Office, LLDP, ADAC	Error setting port vlan membership and tagging or (only for Ip Office script) setting the Data VLAN as management VLAN.	Check existing settings that could be in conflict with the script parameters. Undo settings or boot default the switch, then re-run the script, entering proper data input.

Error setting VLAN Gateway IP address and network mask

Type/Severity	Source	Description	Remedial Action
Information	Run scripts:LLDP, ADAC	IP address conflict.	Check existing settings that could be in conflict with the script parameters. Undo settings or boot default the switch, then re-run the script, entering proper data input.

Comments? infodev@avaya.com

Error setting Voice VLAN Gateway IP address and network mask

Type/Severity	Source	Description	Remedial Action
Information	Run scripts: IP Office, LLDP, ADAC	IP address conflict.	Check existing settings that could be in conflict with the script parameters. Undo settings or boot default the switch, then re-run the script, entering proper data input.

Script was successfully executed

Type/Severity	Source	Description	Remedial Action
Information	Run scripts: IP Office, LLDP, ADAC	Script finished with success.	No action required.

Voice VLAN ID and Data VLAN ID cannot have the same value

Type/Severity	Source	Description	Remedial Action
Information	Run scripts: IP Office, LLDP, ADAC	Voice VLAN and Data VLAN must have different VLAN IDs.	Check existing settings that could be in conflict with the script parameters. Undo settings or boot default the switch, then re-run the script, entering proper data input.

Comments? infodev@avaya.com

Chapter 48: SLPP Messages

SLPP Information Messages

SLPP-guard: hold-down timer has expired on port with SLPP-guard enabled. Port %s has been re-enabled

Type/Severity	Source	Description	Remedial Action
Information	SLPP Guard	The hold-down timer has expired and the port was re-enabled.	No action required.

SLPP-guard: SLPP-guard has not been enabled on port %s as no filters or filter precedences are available to setup an Ethertype filter

Type/Severity	Source	Description	Remedial Action
Information	SLPP Guard	SLPP-guard filters error.	No action required.

SLPP-guard: SLPP packet received on port with SLPP-guard enabled. Port %s has been disabled

Type/Severity	Source	Description	Remedial Action
Information	SLPP Guard	A SLPP packet was received and SLPP-guard disabled the port.	No action required.

Comments? infodev@avaya.com

Chapter 49: SPBM Messages

SPBM Critical Messages

SPBM: ERROR adding i-sid %x to i-sid table - table full

Type/Severity	Source	Description	Remedial Action
Critical	SPBM	The number of I-SIDs that can be configured on the switch is limited.	See the "Limitations" section in the user manual. Remove unneeded I-SIDs.

SPBM: ERROR enabling SPBM due to Software License error

Type/Severity	Source	Description	Remedial Action
Critical	SPBM	SPBM License missing or invalid; IS-IS protocol will not run.	Run **`show license all`** command to check for available licenses. Contact Avaya support.

SPBM Error Messages

SPBM: ERROR adding C-VLAN UNI for i-sid %d, vlan %d - no resources

Type/Severity	Source	Description	Remedial Action
Error	SPBM	UNIs, NNIs and remote nodes use one or more Virtual Ports, depending on the configuration. The number of Virtual Ports that can be configured on the switch is limited.	See the "Limitations" section in the user manual. Remove unneeded UNIs.

SPBM: ERROR adding i-sid %x to i-sid table - table full

Type/Severity	Source	Description	Remedial Action
Critical	SPBM	The number of I-SIDs that can be configured on the switch is limited.	See the "Limitations" section in the user manual. Remove unneeded I-SIDs.

SPBM: ERROR adding NNI on port %d vlan %d - no resources

Type/Severity	Source	Description	Remedial Action
Error	SPBM	UNIs, NNIs and remote nodes use one or more Virtual Ports, depending on the configuration. The number of Virtual Ports that can be configured on the switch is limited.	See the "Limitations" section in the user manual. Remove unneeded UNIs.

Comments? infodev@avaya.com

SPBM: ERROR adding peer %04x.%04x.%04x - no resources

Type/Severity	Source	Description	Remedial Action
Error	SPBM	UNIs, NNIs and remote nodes use one or more Virtual Ports, depending on the configuration. The number of Virtual Ports that can be configured on the switch is limited. The remote system with the system-id listed in the text of the message will not receive.	See the "Limitations" section in the user manual. Remove unneeded UNIs.

SPBM: ERROR adding switched UNI for i-sid %d, port %d, vlan %d - no resources

Type/Severity	Source	Description	Remedial Action
Error	SPBM	UNIs, NNIs and remote nodes use one or more Virtual Ports, depending on the configuration. The number of Virtual Ports that can be configured on the switch is limited.	See the "Limitations" section in the user manual. Remove unneeded UNIs.

SPBM: ERROR adding Transparent UNI for i-sid %d, port %d - no resources

Type/Severity	Source	Description	Remedial Action
Information	SPBM	Error adding Transparent UNI.	No action required.

SPBM: ERROR updating UNI for port %d/%d - no resources

Type/Severity	Source	Description	Remedial Action
Error	SPBM	UNIs, NNIs and remote nodes use one or more Virtual Ports, depending on the configuration. The number of Virtual Ports that can be configured on the switch is limited.	See the "Limitations" section in the user manual. Remove unneeded UNIs.

SPBM: ERROR adding switched UNI for i-sid %d, port %d, vlan %d - no resources

Type/Severity	Source	Description	Remedial Action
Error	SPBM	When a trunk is disabled, the software automatically configures a UNI for each physical port in the trunk. UNIs, NNIs and remote nodes use one or more Virtual Ports, depending on the configuration.	See the "Limitations" section in the user manual. Remove unneeded UNIs.

Comments? infodev@avaya.com

Chapter 50: SFTP messages

SFTP information messages

SSHC ASCII CFG download SFTP failure

Type/Severity	Source	Description	Remedial Action
Information	SSHC (SFTP and SSH Client)	SSHC Client failed to download the ASCII CFG file from SFTP.	Check IP address settings, host reachability, host key existence and username.

SSHC ASCII CFG upload SFTP failure

Type/Severity	Source	Description	Remedial Action
Information	SSHC (SFTP and SSH Client)	SSHC Client failed to upload the ASCII CFG file to SFTP.	Check IP address settings, host reachability, host key existence and username.

SSHC CFG download SFTP failure

Type/Severity	Source	Description	Remedial Action
Information	SSHC (SFTP and SSH Client)	SSHC Client failed to download the CFG file from SFTP.	Check IP address settings, host reachability, host key existence and username.

SSHC CFG upload SFTP failure

Type/Severity	Source	Description	Remedial Action
Information	SSHC (SFTP and SSH Client)	SSHC Client failed to upload the CFG file to SFTP.	Check IP address settings, host reachability, host key existence and username.

SSHC DSA Authentication failure

Type/Severity	Source	Description	Remedial Action
Information	SFTP Client	Failed to authenticate to the SFTP server using the current DSA key as the current public DSA key of the switch/stack was not added to the SFTP server's "authorized keys" list..	Upload the key to TFTP/USB and add it to the server's "authorized keys" list.

SSHC Password Authentication failure

Type/Severity	Source	Description	Remedial Action
Information	SFTP Client	SFTP download/upload operation failed due to incorrect password	Retry operation using the correct password.

SSHC RSA Authentication failure

Type/Severity	Source	Description	Remedial Action
Information	SFTP Client	Failed to authenticate to the SFTP server using the current RSA key as it was not added to the SFTP server's "authorized keys" list..	Upload the key to TFTP/USB and add it to the server's "authorized keys" list.

Comments? infodev@avaya.com

SSHC server connection failure

Type/Severity	Source	Description	Remedial Action
Information	SFTP Client	Failed to connect to SFTP server; following a command involving SFTP.	Check the connectivity to SFTP server. However, this error occurs when you attempt any authentication; it is not caused by authentication failures.

Comments? infodev@avaya.com

Chapter 51: SLA Monitor messages

SLA Monitor Critical Messages

SLAMon Agent message channel creation failure

Type/Severity	Source	Description	Remedial Action
Critical	SLAMon	Internal resource errore — engineering log message	Reset device.

SLAMon Agent platform CLI command interface initialization issue

Type/Severity	Source	Description	Remedial Action
Critical	SLAMon	Internal resource errore — engineering log message	Reset device.

SLAMon Agent platform timer initialization issue

Type/Severity	Source	Description	Remedial Action
Critical	SLAMon	Internal resource errore — engineering log message	Reset device.

SLAMon Agent: terminated

Type/Severity	Source	Description	Remedial Action
Critical	SLAMon	Internal resource error.	Reset device.

SLAMon Agent: terminated - resources unavailable

Type/Severity	Source	Description	Remedial Action
Critical	SLAMon	An internal resource error has occurred.	Reset device

SLAMon Agent: terminated - RTP test exception detected

Type/Severity	Source	Description	Remedial Action
Critical	SLAMon	An internal resource error has occurred.	Reset device

SLAMon Agent: terminated - NTR test exception detected

Type/Severity	Source	Description	Remedial Action
Critical	SLAMon	An internal resource error has occurred.	Reset device

SLAMon Agent: terminated - command/frame processing issue detected

Type/Severity	Source	Description	Remedial Action
Critical	SLAMon	An internal resource error has occurred.	Reset device

Comments? infodev@avaya.com

SLAMon Agent: message channel creation failure

Type/Severity	Source	Description	Remedial Action
Critical	SLAMon	Internal resource error - engineering log message.	Reset device

After agent change message became invalid:

Type/Severity	Source	Description	Remedial Action
Serious/Critical	System Logging	After upgrade/intermediary downgrade, if the Application id or message id are out of range, the message is replaced in order to avoid DAE.	No action required.

SLA Monitor Information Messages

SLAMon Agent CLI support not available

Type/Severity	Source	Description	Remedial Action
Information	SLAMon	SLM CLI support not included in image - current N/A	No action required.

SLAMon Agent CLI timeout value out of range

Type/Severity	Source	Description	Remedial Action
Information	SLAMon	The specified SLA Monitor agent CLI timeout value lies	Specify an in-range value for the agent CLI timeout.

Type/Severity	Source	Description	Remedial Action
		outside the acceptable range (60 seconds to 600 seconds).	

SLAMon Agent disabled

Type/Severity	Source	Description	Remedial Action
Information	SLAMon	SLA Monitor agent state change detected — agent disabled.	No action required.

SLAMon Agent enabled

Type/Severity	Source	Description	Remedial Action
Information	SLAMon	SLA Monitor agent state change detected — agent enabled.	No action required.

SLAMon Agent inconsistent UDP port data specified

Type/Severity	Source	Description	Remedial Action
Information	SLAMon	Agent UDP (command) port and agent-to-agent communication UDP port values conflict with each other. The port values must be unique. Message is also generated when an out-of-range port value is specified and when a port value that conflicts with ports used by other applications (http, https, ssh) is specified.	Utilize defaults or specify unique agent UDP port values.

Comments? infodev@avaya.com

SLAMon Agent info: %d %d %d

Type/Severity	Source	Description	Remedial Action
Information	SLAMon	General debug message — currently N/A	No action required.

SLAMon Agent invalid agent-to-agent port (must be even value)

Type/Severity	Source	Description	Remedial Action
Information	SLAMon	Agent-to-agent communication UDP port must be an even value.	Specify an even value for port.

SLAMon Agent operation is restricted CLI-only

Type/Severity	Source	Description	Remedial Action
Information	SLAMon	The requested operation is only supported through the platform CLI.	Utilize the platform CLI to perform the requested operation.

SLAMon Agent terminated

Type/Severity	Source	Description	Remedial Action
Critical	SLAMon	The agent task logic has been terminated.	System reset required.

SLAMon Agent terminated — command/frame processing issue detected

Type/Severity	Source	Description	Remedial Action
Critical	SLAMon	The agent command/packet receive logic detected an error, causing the agent operation to be terminated.	System reset required.

SLAMon Agent terminated NTR test exception detected

Type/Severity	Source	Description	Remedial Action
Critical	SLAMon	The agent NTR test support detected a failure during test processing, causing agent operation to be terminated.	System reset required.

SLAMon Agent terminated - resources unavailable

Type/Severity	Source	Description	Remedial Action
Critical	SLAMon	Resources required for agent initialization are not available, causing agent operation to be terminated. An invalid configuration, such as when the same port values are specified for agent-server and agent-agent communication, can also impact resource availability.	System reset required.

Comments? infodev@avaya.com

SLAMon Agent terminated - RTP test exception detected

Type/Severity	Source	Description	Remedial Action
Critical	SLAMon	The agent RTP test support detected a failure during test processing, causing agent operation to be terminated.	System reset required.

Comments? infodev@avaya.com

Chapter 52: SMLT messages

SMLT information messages

SLPP Warning - PDU was received on Vlan VlanId Unit UnitNo Port PortNo .

Type/Severity	Source	Description	Remedial Action
Information	SMLT	The system detected an SLPP error when the SLPP packet sent is received back on a different VLAN.	Check for the correct port configuration

SMLT IMC invalid cmd 1– StkCmd

Type/Severity	Source	Description	Remedial Action
Information	SMLT	An invalid SMLT Imc command received in the stack.	Restart the system.

SMLT IMC tx error

Type/Severity	Source	Description	Remedial Action
Information	SMLT	The system failed to transmit the IMC message in the stack.	Restart the system.

SMLT input parameter error mlt port vlan

Type/Severity	Source	Description	Remedial Action
Information	SMLT	The system failed to enable the SMLT as the IST ports are not a part of the VLAN.	Check for the correct VLAN membership of the IST ports.

SMLT Stack db ex event num -0 –0*22221111

Type/Severity	Source	Description	Remedial Action
Information	SMLT	Log SMLT db exchange events.	No action required.

SMLT stackEventNotify Invalid Msg Cmd - 0 – 0

Type/Severity	Source	Description	Remedial Action
Information	SMLT	The system received an invalid stack related event.	Restart the system.

SMLT Stack inactive event 0-0- modMask

Type/Severity	Source	Description	Remedial Action
Information	SMLT	Log SMLT unit inactive events.	No action required.

SMLT Stack joined event num - 0 – 0*33331111

Type/Severity	Source	Description	Remedial Action
Information	SMLT	Log SMLT stack Join events.	No action required.

Comments? infodev@avaya.com

SMLT Stack leaved event 0 - 0 - modMask

Type/Severity	Source	Description	Remedial Action
Information	SMLT	Log SMLT stack leave events.	No action required.

SMLT STP enabled on IST trunk trkNo stp group grp

Type/Severity	Source	Description	Remedial Action
Information	SMLT	STP enabled on the IST trunk error.	Disable the STP on IST trunk ports.

SMLT Warning - LAC SMLT with more than 8 links - key - count

Type/Severity	Source	Description	Remedial Action
Information	SMLT	LAC/SMLT with more than 8 links with specified key count.	Do not configure more than 8 links in the SMLT over the LAC configuration.

SMLT Warning - smltEnable Software License Error- 0 – 0

Type/Severity	Source	Description	Remedial Action
Information	SMLT	This is a SMLT related warning indicating, software License error.	Check if a valid software license is available.

SMLT Warning - SMLT mismatched Lac_Sys_ID error shutdown all SMLT lac po

Type/Severity	Source	Description	Remedial Action
Information	SMLT	This is an SMLT related warning indicating, SMLT system ID mismatch.	The SMLT system ID did not match. Configure the correct system ID.

Comments? infodev@avaya.com

Chapter 53: SNMP Server messages

SNMP Server warning messages

Trap: FCoE - Egress Issue Detected

Type/Severity	Source	Description	Remedial Action
Serious	FCoE Redirect	Issue detected with link/trunk used for FCoE Redirect.	Check FCoE config/ link status.

Trap s5CtrUnitDown

Type/Severity	Source	Description	Remedial Action
Serious	L3, MLT	Unit down.	No action required.

Trap: slaMonitorAgentExceptionDetected

Type/Severity	Source	Description	Remedial Action
Critical	SLAMon	SLAMon agent operation terminated.	Reset device.

SNMP Server information messages

Authentication Failure Trap

Type/Severity	Source	Description	Remedial Action
Information	SNMP	Authentication Failure.	No action required.

BPDU received on port with BPDU-Filtering enabled.

Type/Severity	Source	Description	Remedial Action
Information	STP	BPDU received on port with BPDU-Filtering enabled.	No action required.

Cold Start Trap

Type/Severity	Source	Description	Remedial Action
Information	SNMP	Cold Start	No action required.

DAI ARP packet with invalid IP MAC binding dropped on untrusted port unit# port#

Type/Severity	Source	Description	Remedial Action
Information	DAI	ARP packet ingressed on a DAI untrusted port with a hardware MAC address and IP address does not match any entries in the DHCP binding table. This violates the DAI integrity check and the packet is dropped.	Isolate the offender.

Comments? infodev@avaya.com

DHCP Snoop DHCP ACK dropped on untrusted port unit# port# (not allowed on untrusted port)

Type/Severity	Source	Description	Remedial Action
Information	DHCPSNOOP	DHCP ACK reply packet ingressed on an DHCP Snoop untrusted port. This violates the DHCP Snoop integrity check and the packet is dropped.	Isolate the offender.

DHCP Snoop DHCP binding table is full additional DHCP clients will not be added to the binding table

Type/ Severity	Source	Description	Remedial Action
Information	DHCPSNOOP	The maximum number of DHCP binding entries (1024) is reached. Any additional DHCP client entries will not be added to the binding table.	Scale down the number of DHCP clients.

DHCP Snoop: DHCP DISCOVER dropped on port %d/%d (source MAC not matching client MAC)

Parameters	Type/ Severity	Source	Description	Remedial Action
Source MAC address Client MAC address	Information	DHCPSNOOP	A DHCP Discover packet was received on port %d/%d but the source MAC Address did not match the client MAC address.	Check the sending client. It may be an intrusion.

DHCP Snoop DHCP NAK dropped on untrusted port unit# port# (not allowed on untrusted port)

Type/Severity	Source	Description	Remedial Action
Information	DHCPSNOOP	DHCP NAK reply packet ingressed on an DHCP Snoop untrusted port. This violates the DHCP Snoop integrity check and the packet is dropped.	Isolate the offender.

DHCP Snoop DHCP OFFER dropped on untrusted port unit# port# (not allowed on untrusted port)

Type/Severity	Source	Description	Remedial Action
Information	DHCPSNOOP	DHCP OFFER reply packet ingressed on an DHCP Snoop untrusted port. This violates the DHCP Snoop integrity check and the packet is dropped.	Isolate the offender.

DHCP Snoop DHCP RELEASE DECLINE dropped on untrusted port unit# port# because MAC Addr(MACaddress) is associated to port unit# port#

Type/Severity	Source	Description	Remedial Action
Information	DHCPSNOOP	DHCP RELEASE or DECLINE packet with the DHCP client hardware MAC address and client port from the binding table ingressed on a different DHCP Snoop untrusted port. This violates the	Isolate the offender.

Comments? infodev@avaya.com

Type/Severity	Source	Description	Remedial Action
		DHCP Snoop integrity check and the packet is dropped.	

DHCP Snoop DHCP RELEASE DECLINE dropped on untrusted port unit# port# (MAC Addr(MACaddress) does not exist in binding table)

Type/Severity	Source	Description	Remedial Action
Information	DHCPSNOOP	DHCP RELEASE or DECLINE packet with the DHCP client hardware MAC address is not found in the binding table ingressed on a DHCP Snoop untrusted port. This violates the DHCP Snoop integrity check and the packet is dropped.	Isolate the offender.

DHCP Snoop: DHCP packet dropped on port %d/%d - static entry with the same MAC %02x-%02x-%02x-%02x-%02x-%02x in binding table

Type/Severity	Source	Description	Remedial Action
Information	SNMP	Drop static entry.	No action required.

DHCP Snoop DHCP snooping binding table restored successfully from TFTP address

Type/Severity	Source	Description	Remedial Action
Information	DHCP SNOOP	External-save/restore was unsuccessful.	Check TFTP connection or the USB target for availability.

DHCP Snoop DHCP snooping binding table restored successfully from USB unit unit#

Type/Severity	Source	Description	Remedial Action
Information	DHCP SNOOP	External-save/restore was unsuccessful on the mentioned target.	Check TFTP connection or the USB target for availability.

DHCP Snoop DHCP snooping binding table restore from TFTP address A.B.C.D IPv6_address failed

Type/Severity	Source	Description	Remedial Action
Information	DHCP SNOOP	External-save/restore was unsuccessful on the mentioned target.	Check TFTP connection or the USB target for availability.

DHCP Snoop DHCP snooping binding table restore from USB unit unit# failed

Type/Severity	Source	Description	Remedial Action
Information	DHCP SNOOP	External-save/restore was unsuccessful.	Check TFTP connection or the USB target for availability.

DHCP Snoop DHCP snooping binding table saved successfully to TFTP address

Type/Severity	Source	Description	Remedial Action
Information	DHCP SNOOP	External-save/restore occurred successfully on the mentioned target.	No action required.

Comments? infodev@avaya.com

DHCP Snoop: DHCP snooping binding table save to TFTP address, failed

Type/Severity	Source	Description	Remedial Action
Information	DHCPSNOOP	External-save/restore occurred successfully on the mentioned target.	No action required.

DHCP Snoop DHCP snooping binding table saved successfully to USB unit unit#

Type/ Severity	Source	Description	Remedial Action
Information	DHCP SNOOP	External-save/restore occurred successfully on the mentioned target.	No action required.

DHCP Snoop DHCP snooping binding table save to USB unit unit# failed

Type/Severity	Source	Description	Remedial Action
Information	DHCP SNOOP	External-save/restore occurred successfully on the mentioned target.	No action required.

DHCP Snoop: DHCP snooping entry with MAC %02x-%02x-%02x-%02x-%02x-%02x not restored (invalid Vlan %d)

Type/Severity	Source	Description	Remedial Action
Information	DHCP SNOOP	External-save entry could not be restored due to an invalid VLAN.	Compare external entry VLAN against currently configured VLANs and

Type/Severity	Source	Description	Remedial Action
			change configuration if necessary.

DHCP Snoop DHCP snooping entry entry number not restored due to MAC conflict

Type/Severity	Source	Description	Remedial Action
Information	DHCP SNOOP	Binding entry could not be restored due to MAC conflict.	No action required.

DHCP Snoop DHCP snooping entry entry number not restored due to expired lease

Type/Severity	Source	Description	Remedial Action
Information	DHCP SNOOP	Binding entry could not be restored as the lease expired.	No action required.

DHCP Snoop DHCP snooping entry with MAC MacAddress not restored on invalid interface unit# port#

Type/Severity	Source	Description	Remedial Action
Information	DHCP SNOOP	Binding entry could not be restored due to an invalid interface (unit/ port combination read from external file is no longer available or invalid altogether).	Check the unit/port combinations in the external-save file with your actual topology, and modify the external-save file if necessary.

Comments? infodev@avaya.com

DHCP Snoop DHCP snooping entry entry number not restored due to parsing failure

Type/Severity	Source	Description	Remedial Action
Information	DHCP SNOOP	Binding entry could not be restored due to various parsing failures.	Check and modify the external-save file for unexpected modifications in entry syntax.

DHCP Snoop NTP is not synchronized; external save restore of DHCP snooping entries not possible

Type/Severity	Source	Description	Remedial Action
Information	DHCP SNOOP	The external actions (Restore or Save) not possible, as the Unit (S)NTP server is not synchronized.	Make sure time source is properly set to (S)NTP and the server is synchronized.

Egp Neighbor Loss Trap

Type/Severity	Source	Description	Remedial Action
Information	SNMP	Egp Neighbor Loss.	No action required.

Enterprise Specific Trap

Type/Severity	Source	Description	Remedial Action
Information	SNMP	Enterprise Specific Trap.	No action required.

IPSG Insufficient resources available to enable IPSG on port unit# port#

Type/ Severity	Source	Description	Remedial Action
Information	IPSG	Insufficient resources available to enable IPSG on port.	No action required.

IPSG Maximum IP entries on port unit# port# has been reached

Type/Severity	Source	Description	Remedial Action
Information	IPSG	Maximum IP entries on port has been reached.	Scale down the number of IP entries on port.

Link Down Trap

Type/Severity	Source	Description	Remedial Action
Information	IFMGR, SNMP	Link Down.	No action required.

Link Up Trap

Type/Severity	Source	Description	Remedial Action
Information	IFMGR, SNMP	Link up.	No action required.

Comments? infodev@avaya.com

PIM Neighbor status change Up

Type/Severity	Source	Description	Remedial Action
Information	PIM	PIM_NBR_UP: A new neighbor is detected, This occurs when a PIM Hello message is received from an active PIM router. This may result in change in IP multicast traffic flow if this neighbor is towards RP or BSR espcially if combined with change in unicast routing.	If the same neighbor is repeatedly appearing and disappearing, this is due to congestion in the link towards this neighbor. Check if unicast routing and CPU utilization is also being affected.

PIM Neighbor status change Down

Type/Severity	Source	Description	Remedial Action
Information	PIM	PIM_NBR_DOWN: An existing neighbor has timed out. This occurs when PIM Hello messages are not received from a neighbor within 3.5 times the query interval for an active PIM interface. This may lead to changes in the IP Multicast traffic flow.	Check if the neighbor router is functional and is sending out PIM Hellos.

Radius: Server with index %d is down

Parameters	Type/ Severity	Source	Description	Remedial Action
Server Index	Information	Radius	Radius server is down.	Check connectivity with server.

Radius: Server with index %d is up

Parameters	Type/ Severity	Source	Description	Remedial Action
Server Index	Information	Radius	Radius server is up	No action required.

SPBM adjacency with neighbor

Type/Severity	Source	Description	Remedial Action
Information	ISIS	When IS-IS forms more than 1 adjacency with the same IS.	No action required.

SPBM detect adj

Type/Severity	Source	Description	Remedial Action
Information	ISIS	When the IS-IS adjacency state changes (down, init, up).	No action required.

SPBM ISIS

Type/Severity	Source	Description	Remedial Action
Information	ISIS	An IS-IS trap indicating that a Hello packet with a duplicate system-id has been received.	Correct IS-IS system-id configuration.

Comments? infodev@avaya.com

SPBM ISIS detect duplicate nick-name

Type/Severity	Source	Description	Remedial Action
Information	ISIS	An IS-IS trap indicating that a LSP with a duplicate nickname has received.	Correct IS-IS SPBM nick-name configuration.

SPBM ISIS node

Type/Severity	Source	Description	Remedial Action
Information	ISIS	An IS-IS trap was sent indicating that a LSP with a different value of I1-metric has been received	Correct SPBM I1-metric configuration.

Trap bsAdacPortConfigNotification

Type/Severity	Source	Description	Remedial Action
Information	ADAC	ADAC Port Configuration.	No action required.

Trap bsAdacPortOperDisabledNotification

Type/Severity	Source	Description	Remedial Action
Information	ADAC	ADAC Port operation disabled.	No action required.

Trap bsnConfigurationSavedToNvram

Type/Severity	Source	Description	Remedial Action
Information	CONFIG DATA	The configuration is saved to NVRAM.	No action required.

Trap: bsDhcpSnoopingExtSaveSFTPSyncSuccess

Type/Severity	Source	Description	Remedial Action
Information	SNMP	This notification is generated after successfully saving the DHCP snooping binding table to a SFTP server external file.	No action required.

Trap bsnEapAccessViolation

Type/Severity	Source	Description	Remedial Action
Information	EAP	EAP access violation.	No action required.

Trap bsnEapUbpFailure

Type/Severity	Source	Description	Remedial Action
Information	EAP	EAP UBP failure.	No action required.

Comments? infodev@avaya.com

Trap bsnLacPortDisabledDueToLossOfVLACPDU

Type/Severity	Source	Description	Remedial Action
Information	LAC	Lac Port Disabled Due To Loss Of VLACPDU	No action required.

Trap bsnLacPortEnabledDueToReceiptOfVLACPDU

Type/Severity	Source	Description	Remedial Action
Information	LAC	LAC Port Enabled as the VLACPDU was received.	No action required.

Trap: bsnROPasswordExpired: Read-only password expired

Type/Severity	Source	Description	Remedial Action
Information	Password Security	Notify user that local read-only password has expired.	No action Required

Trap: bsnRWPasswordExpired: Read-write password expired

Type/Severity	Source	Description	Remedial Action
Information	Password Security	Notify user that local read-write password has expired.	No action required.

Trap: bsnSFPInsertion on port

Type/Severity	Source	Description	Remedial Action
Information	SNMP	SFP was inserted.	No action required.

Trap: bsnSFPRemoval on port

Type/Severity	Source	Description	Remedial Action
Information	SNMP	SFP was removed.	No action required.

Trap bsnStackConfigurationError

Type/Severity	Source	Description	Remedial Action
Information	STK MONITOR	Stack Configuration Error.	No action required.

Trap bsnStackManagerReconfiguration

Type/Severity	Source	Description	Remedial Action
Information	STKMGR	Stack manager re-configuration.	No action required.

Trap: bsnSystemUp365Days sent from unit %d

Parameters	Type/ Severity	Source	Description	Remedial Action
Unit	Information	TOTAL SYS UPTIME (TSU)	The message is logged with the SNMP trap. The notification indicates the system has been up for 365 days.	No action required

Comments? infodev@avaya.com

Trap bsnTrialLicenseExpiration Trial license license# has expired. Disable licensed features to avoid network interruption

Type/Severity	Source	Description	Remedial Action
Information	SOFTLIC	The trial license has expired.	Disable the licensed features to avoid network interruption.

Trap bsnTrialLicenseExpiration Trial license license# will expire in # days day(s)

Type/Severity	Source	Description	Remedial Action
Information	SOFTLIC	This message indicates that the trial license will expire.	No action required.

Trap bspePethPsePortCurrentStatusNotification

Type/Severity	Source	Description	Remedial Action
Information	POL	Peth Pse Port Current Status.	No action required.

Trap bsUnicastStormControlAboveHighWatermark

Type/Severity	Source	Description	Remedial Action
Information	DRIVER	Unicast Storm Control reached the high watermark level.	No action required.

Trap bsUnicastStormControlBelowLowWatermark

Type/Severity	Source	Description	Remedial Action
Information	DRIVER	Unicast Storm Control has gone below low watermark level.	No action required.

Trap: bsnUSBInsertion on unit

Type/Severity	Source	Description	Remedial Action
Information	SNMP	USB was inserted.	No action required.

Trap: bsnUSBRemoval on unit

Type/Severity	Source	Description	Remedial Action
Information	SNMP	USB was removed.	No action required.

Trap bsveVrrpTrapStateTransition

Type/Severity	Source	Description	Remedial Action
Information	VRRP	VRRP Trap State Transition.	No action required.

Trap DAPP - DoS Attack Detected

Type/Severity	Source	Description	Remedial Action
Information	QPAV2	The system detected a DAPP - DoS attack.	No action required.

Comments? infodev@avaya.com

Trap Device has entered Forced Stack Mode (MAC Address)

Type/Severity	Source	Description	Remedial Action
Information	IPT	Device has entered Forced Stack Mode.	No action required.

Trap entConfigChange

Type/Severity	Source	Description	Remedial Action
Information	ENTMIB	Ent Config Change.	No action required.

Trap fallingAlarm

Type/Severity	Source	Description	Remedial Action
Information	RMON	Falling Alarm.	No action required.

Trap lldpRemTableChange Ageouts = count

Type/Severity	Source	Description	Remedial Action
Information	802.1AB	lldpRemTableChange Ageouts Number	No action required.

Trap lldpRemTableChange Deletes = count

Type/Severity	Source	Description	Remedial Action
Information	802.1AB	lldpRemTableChange Deletes Number.	No action required.

Trap lldpRemTableChange Drops = count

Type/Severity	Source	Description	Remedial Action
Information	802.1AB	lldpRemTableChange Drops Number	No action required.

Trap lldpRemTableChange Inserts = count

Type/Severity	Source	Description	Remedial Action
Information	802.1AB	lldpRemTableChange Inserts Number	No action required.

Trap lldpXMedTopologyChangeDetected Subtype = subtype Class = class

Type/Severity	Source	Description	Remedial Action
Information	802.1AB	The system detected a LldpXMed Topology Change.	No action required.

Trap newRoot

Type/Severity	Source	Description	Remedial Action
Information	NNCLI	New root.	No action required.

Trap ntnQosPolicyEvolLocalUbpSessionFailure

Type/Severity	Source	Description	Remedial Action
Information	QPAV2	QoS Policy Evol Local UBP Session Failed.	No action required.

Comments? infodev@avaya.com

Trap ospfIfAuthFailure

Type/Severity	Source	Description	Remedial Action
Information	OSPF	The OSPF Interface Authentication failed.	No action required.

Trap ospfIfConfigError

Type/Severity	Source	Description	Remedial Action
Information	OSPF	OSPF Interface Configuration Error.	No action required.

Trap ospfIfStateChange

Type/Severity	Source	Description	Remedial Action
Information	OSPF	The OSPF Interface state changed.	No action required.

Trap ospfNbrStateChange

Type/Severity	Source	Description	Remedial Action
Information	OSPF	OSPF Neighbor State Change.	No action required.

Trap ospfVirtIfAuthFailure

Type/Severity	Source	Description	Remedial Action
Information	OSPF	The OSPF Virtual Interface Authentication failed.	No action required.

Trap ospfVirtIfConfigError

Type/Severity	Source	Description	Remedial Action
Information	OSPF	The system detected an OSPF Virtual Interface Configuration Error.	No action required.

Trap ospfVirtIfStateChange

Type/Severity	Source	Description	Remedial Action
Information	OSPF	OSPF Virtual Interface State Change.	No action required.

Trap ospfVirtNbrStateChange

Type/Severity	Source	Description	Remedial Action
Information	OSPF	OSPF Virtual Neighbor State Change.	No action required.

Trap pethMainPowerUsageOffNotification

Type/Severity	Source	Description	Remedial Action
Information	POL	Peth Main Power Usage Off.	No action required.

Trap pethMainPowerUsageOnNotification

Type/Severity	Source	Description	Remedial Action
Information	POL	Peth Main Power Usage On.	No action required.

Comments? infodev@avaya.com

Trap pethPsePortOnOffNotification

Type/Severity	Source	Description	Remedial Action
Information	POL	Peth Pse Port On Off.	No action required.

Trap: rclsisPlsbBvidMismatchTrap

Type/Severity	Source	Description	Remedial Action
Information	ISIS	Trap was sent when the B-VID TLV from a neighbor node does not match the local configuration.	Correct SPBM B-VID configuration.

Trap: rclsisPlsbLsdbUpdateTrap

Type/Severity	Source	Description	Remedial Action
Information	ISIS	An IS-IS trap indicating that LSDB information has changed.	No action required.

Trap risingAlarm

Type/Severity	Source	Description	Remedial Action
Information	RMON	Rising alarm.	No action required.

Trap RSTP Error Event

Type/Severity	Source	Description	Remedial Action
Information	NNRST	RSTP Error Event.	No action required.

Trap RSTP General Event

Type/Severity	Source	Description	Remedial Action
Information	NNRST	RSTP General Event.	No action required.

Trap RSTP New Root

Type/Severity	Source	Description	Remedial Action
Information	NNRST	RSTP New Root.	No action required.

Trap RSTP Protocol Migration

Type/Severity	Source	Description	Remedial Action
Information	NNRST	RSTP Protocol Migration.	No action required.

Trap RSTP Topology Change

Type/Severity	Source	Description	Remedial Action
Information	NNRST	RSTP Topology Change.	No action required.

Trap: Run %s %s

Type/Severity	Source	Description	Remedial Action
Information	SNMP	Script %s failed/was successfully executed.	No action required.

Comments? infodev@avaya.com

Trap s5CtrUnitDown

Type/Severity	Source	Description	Remedial Action
Warning	L3, MLT	Unit down.	No action required.

Trap s5EtrSbsMacAccessViolation

Type/ Severity	Source	Description	Remedial Action
Information	BAYSECURE, DCE	MAC access violation.	No action required.

Trap s5EtrSbsMacAccessViolation

Type/ Severity	Source	Description	Remedial Action
Information	BAYSECURE, DCE	MAC access violation.	No action required.

Trap s5EtrSbsMacRemoved

Type/Severity	Source	Description	Remedial Action
Information	NNCLI	MAC removed.	No action required.

Trap s5EtrSbsMacTableCleared

Type/Severity	Source	Description	Remedial Action
Information	NNCLI	MAC Table Cleared.	No action required.

Trap s5EtrSbsMacTableClearedForPort

Type/Severity	Source	Description	Remedial Action
Information	NNCLI	The MAC table cleared for the Port.	No action required.

Trap SLPP Port Down Event

Type/Severity	Source	Description	Remedial Action
Information	SMLT	SLPP Port Down Event.	No action required.

Trap Smlt Ist Link Down

Type/Severity	Source	Description	Remedial Action
Information	SMLT	SMLT IST Link Down.	No action required.

Trap Smlt Ist Link Up

Type/Severity	Source	Description	Remedial Action
Information	SMLT	SMLT IST Link Up	No action required.

Trap Smlt Link Down

Type/Severity	Source	Description	Remedial Action
Information	SMLT	SMLT Link Down.	No action required.

Comments? infodev@avaya.com

Trap Smlt Link Up

Type/Severity	Source	Description	Remedial Action
Information	SMLT	SMLT Link Up.	No action required.

Trap s5CtrHotSwap

Type/Severity	Source	Description	Remedial Action
Information	MCMGR, DRPMGR	Hot Swap.	No action required.

Trap topologyChange

Type/Severity	Source	Description	Remedial Action
Information	NNCLI	Topology Change.	No action required.

Trap ubpEAPSessionEnd

Type/Severity	Source	Description	Remedial Action
Information	QPAV2	EAP Session end.	No action required.

Trap ubpEAPSessionStart

Type/Severity	Source	Description	Remedial Action
Information	QPAV2	EAP Session Start.	No action required.

Trap vrrpTrapNewMaster

Type/Severity	Source	Description	Remedial Action
Information	VRRP	VRRP Trap New Master.	No action required.

Trap: s5CtrFanDirectionError

Type/Severity	Source	Description	Remedial Action
Information	DCE	The message is logged with the SNMP trap s5CtrFanDirectionError. This notification indicates that a fan component's direction is incorrect.	Verify the fan component's direction.

Trap: s5CtrHighTemperatureError

Type/Severity	Source	Description	Remedial Action
Information	DCE	The message is logged with the SNMP trap s5CtrHighTemperatureError. This notification indicates that the system is overheated.	Verify system temperature.

Trap: s5EtrMacAddressTablesThresholdReached

Type/Severity	Source	Description	Remedial Action
Information	CDT	s5EtrMacAddressTablesThresholdReached trap signifies that the MAC address tables threshold is reached.	Remove at least one MAC address.

Comments? infodev@avaya.com

Trap: rclsisPlsbSmltVirtBmacMismatchTrap

Type/Severity	Source	Description	Remedial Action
Information	SPB	A PLSB ISIS trap signifies that the Virtual BMAC configured in the switch is different from virtual BMAC configured in the IST peer.	No action required.

Trap: rclsisPlsbSmltPeerBmacMismatchTrap

Type/Severity	Source	Description	Remedial Action
Information	SPB	A PLSB ISIS trap signifies that the Smlt Split-Beb configured in the local switch and IST peer are the same. Configure One IST switch as Split-Beb primary and configure IST peer as Split-Beb secondary.	No action required.

Trap: rclsisPlsbSmltSplitBebMismatchTrap

Type/Severity	Source	Description	Remedial Action
Information	SBR	A PLSB ISIS trap signifies that the Smlt Split-Beb configured in the local switch and IST peer are same. Configure One IST switch as Split-Beb primary and configure IST peer as Split-Beb secondary.	No action required.

Trap: bsLstInterfaceStatusChanged

Type/Severity	Source	Description	Remedial Action
Information	LST	This notification is generated when a physical or logical interface changes its status in a particular link-state tracking group.	No action required.

Trap: bsLstGroupOperStateChanged

Type/Severity	Source	Description	Remedial Action
Information	LST	This notification is generated when the operational status of a link-state tracking group changes due to an interface status change.	No action required.

Trap: bsDhcpSnoopingExtSaveSFTPSyncSuccess

Type/Severity	Source	Description	Remedial Action
Warning/ Information	Baysecure	Maximum number of MAC addresses that can be learned on a trunk is reached.	No action required.

Trap: bsDhcpSnoopingExtSaveSFTPSyncFailure

Type/Severity	Source	Description	Remedial Action
Information	DHCPSNOOP	This notification is generated after unsuccessfully saving the DHCP Snooping binding	No action required.

Comments? infodev@avaya.com

Type/Severity	Source	Description	Remedial Action
		table to a SFTP server external file.	

Trap: bsDhcpSnoopingExtSaveSFTPRestoreSuccess

Type/Severity	Source	Description	Remedial Action
Information	DHCPSNOOP	This notification is generated after successfully restoring the DHCP snooping binding table from a SFTP server external file.	No action required.

Trap: bsDhcpSnoopingExtSaveSFTPRestoreFailure

Type/Severity	Source	Description	Remedial Action
Information	DHCPSNOOP	This notification is generated after unsuccessfully restoring the DHCP snooping binding table from a SFTP server external file.	No action required.

DHCP Snoop: DHCP snooping entry with MAC %02x-%02x-%02x-%02x-%02x-%02x not restored on trusted interface %d/%d

Type/Severity	Source	Description	Remedial Action
Information	DHCPSNOOP	The message is logged with the SNMP trap bsDhcpSnoopingExtSaveEntryIfTrustedConflict. This notification is generated when a DHCP snooping binding entry failes to restore from an	No action required.

Type/Severity	Source	Description	Remedial Action
		external file on a trusted interface.	

Comments? infodev@avaya.com

Chapter 54: SNTP messages

SNTP critical messages

SNTP Could not sync to NTP servers.

Type/Severity	Source	Description	Remedial Action
Critical	SNTP	The SNTP could not synchronize with any of the two NTP servers.	Try synchronizing to a valid NTP server. Make sure that the SNTP is connected to the NTP servers you are trying to synchronize with.

SNTP information messages

SNTP: First synchronization successful.

Type/Severity	Source	Description	Remedial Action
Information	SNTP	The SNTP is synchronized with one of the NTP servers.	No action required.

Comments? infodev@avaya.com

Chapter 55: SSH messages

SSH information messages

SSHC: ASCII CFG download SFTP failure

Type/Severity	Source	Description	Remedial Action
Information	SFTP	Download of ASCII config file to SFTP failed.	Check IP address settings, host reachability, host key existence and username.

SSHC: ASCII CFG upload SFTP failure

Type/Severity	Source	Description	Remedial Action
Information	SFTP	Upload of ASCII config file to SFTP failed.	Check IP address settings, host reachability, host key existence and username.

SSH_CLIENT Key couldnt be saved for host ip address

Type/Severity	Source	Description	Remedial Action
Information	SSH Client	New host's key could not be saved as NVRAM is full or defective.	Remove other host's keys to create space on NVRAM, and try again.

SSH CLIENT SSH Connection to IP ip address was closed because parent console session console session ID was closed

Type/Severity	Source	Description	Remedial Action
Information	SSH Client	SSH Connection is closed as the console session, from which SSH Client was launched closed. (for example, ssh DUT, then ssh PC, then close ssh to DUT session)	No action required.

SSH CLIENT SSH Connection to %s was disconnected

Type/Severity	Source	Description	Remedial Action
Information	SSH Client	Successfully disconnected the SSH connection.	No action required.

SSH CLIENT: SSH Connection to %s was disconnected by host. Connection time: %s

Type/Severity	Source	Description	Remedial Action
Information	SSH Client	Host disconnected the SSH connection.	No action required.

SSH CLIENT: SSH Connection to %s was disconnected by user. Connection time: %s.

Type/Severity	Source	Description	Remedial Action
Information	SSH Client	SSH user ended SSH connection.	No action Required.

Comments? infodev@avaya.com

SSH CLIENT Successful SSH Connection to %s using %s authentication

Type/Severity	Source	Description	Remedial Action
Information	SSH Client	Successful SSH Connection.	No action required.

SSH disabled

Type/Severity	Source	Description	Remedial Action
Information	SSH	The SSH is disabled	No action required.

SSH DSA key deleted

Type/Severity	Source	Description	Remedial Action
Information	SSH	The SSH DSA key deleted.	No action required.

SSH DSA KEY generation completed

Type/Severity	Source	Description	Remedial Action
Information	SSH	The SSH DSA key generation completed.	No action required.

SSH enabled in non-secure mode

Type/Severity	Source	Description	Remedial Action
Information	SSH	The SSH is enabled in a non-secure mode.	No action required.

SSH enabled in secure mode

Type/Severity	Source	Description	Remedial Action
Information	SSH	The SSH is enabled in the secure mode.	No action required.

SSH Maximum number of ssh sessions has been reached

Type/Severity	Source	Description	Remedial Action
Information	SSH	The maximum number of SSH session is reached.	No action required.

SSH RSA KEY generation completed

Type/Severity	Source	Description	Remedial Action
Information	SSH	The SSH RSA key is successfully generated.	No action required.

SSH RSA key overwritten

Type/Severity	Source	Description	Remedial Action
Information	SSH	The SSH RSA key is overwritten.	No action required.

SSH session login using port

Type/Severity	Source	Description	Remedial Action
Information	SSH	Login session.	No action required.

Comments? infodev@avaya.com

SSH System is generating DSA KEY wait ...

Type/Severity	Source	Description	Remedial Action
Information	SSH	The system is generating the DSA key.	No action required.

SSH TFTP DSA key download complete

Type/Severity	Source	Description	Remedial Action
Information	SSH	Download the SSH DSA key through the completed TFTP.	No action required.

SSH TFTP RSA key download complete

Type/Severity	Source	Description	Remedial Action
Information	SSH	SSH RSA key is successfully downloaded through TFTP.	No action required.

SSH USB DSA key download complete

Type/Severity	Source	Description	Remedial Action
Information	SSH	The SSH DSA key downloading through the USB is completed.	No action required.

SSH USB RSA key download complete

Type/Severity	Source	Description	Remedial Action
Information	SSH	The SSH RSA key is successfully downloaded through the USB.	No action required.

SSH session closed by ip address remote host. Connection time h hours m minutes

Type/Severity	Source	Description	Remedial Action
Information	SSH Client	Remote host closed the SSH session.	No action required.

Successful SSH connection to ip address

Type/Severity	Source	Description	Remedial Action
Information	SSH Client	SSH connection completed successfully.	No action required.

Comments? infodev@avaya.com

Chapter 56: SSHC messages

SSHC information messages

SSHC: CFG download SFTP failure

Type/Severity	Source	Description	Remedial Action
Information	SSH Client	Communication with server failed for some reason, therefore download failed.	Check if ping works (if not dropped by firewall) for SFTP server If full path is used verify if the path exist on the server. Check the server settings for sshd/sftp.

SSHC: CFG upload SFTP failure

Type/Severity	Source	Description	Remedial Action
Information	SSH Client	Communication with server failed for some reason, therefore upload failed.	Check if ping works (if not dropped by firewall) for SFTP server If full path is used verify if the path exist on the server. Check the server settings for sshd/sftp.

SSHC DSA key generation failure

Type/Severity	Source	Description	Remedial Action
Information	SSHC (SFTP and SSH Client)	SSHC Client failed to generate the DSA key.	No action required.

SSHC DSA key save failure

Type/Severity	Source	Description	Remedial Action
Information	SSHC (SFTP and SSH Client)	SSHC Client failed to save the DSA key.	No action required.

SSHC DSA key upload TFTP failure

Type/Severity	Source	Description	Remedial Action
Information	SSHC (SFTP and SSH Client)	SSHC Client failed to upload the DSA key to TFTP.	Check the TFTP server connection, and try again.

SSHC DSA key upload USB failure

Type/Severity	Source	Description	Remedial Action
Information	SSHC (SFTP and SSH Client)	SSHC Client failed to upload the DSA key to the USB as, the memory stick is full or corrupted.	Create space on memory stick or replace the memory stick, and try again.

Comments? infodev@avaya.com

SSHC: Password Authentication failure

Type/Severity	Source	Description	Remedial Action
Information	SSH Client	Wrong username or password used, or password exceeded 30 characters.	Check if user and password are correct and have 30 or less characters.

SSHC: RSA Authentication failure

Type/Severity	Source	Description	Remedial Action
Information	SSH Client	Mismatch or inconsistency between the generated key and the key uploaded on server.	Check if the DSA/RSA key was handled correctly. If not sure regenerate the key and upload the new key using tftp server and then try again.

SSHC RSA key generation failure

Type/Severity	Source	Description	Remedial Action
Information	SSHC (SFTP and SSH Client)	SSHC Client failed to generate the RSA.	No action required.

SSHC RSA key save failure

Type/Severity	Source	Description	Remedial Action
Information	SSHC (SFTP and SSH Client)	SSHC Client failed to save the RSA key.	No action required.

SSHC RSA key upload TFTP failure

Type/Severity	Source	Description	Remedial Action
Information	SSHC (SFTP and SSH Client)	SSHC Client failed to upload the RSA key to TFTP.	Check TFTP server connection, and try again.

SSHC RSA key upload USB failure

Type/Severity	Source	Description	Remedial Action
Information	SSHC (SFTP and SSH Client)	SSHC Client failed to upload the RSA key to the USB as, the memory stick is full or corrupted.	Create space on memory stick or replace the memory stick, and try again.

Comments? infodev@avaya.com

Chapter 57: SSL messages

SSL information messages

SSL certificate creation completed

Type/Severity	Source	Description	Remedial Action
Information	SSL	SSL certificate creation completed.	No action required.

SSL certificate creation failed

Type/Severity	Source	Description	Remedial Action
Information	SSL	SSL certificate creation failed.	Retry.

SSL certificate deleted

Type/Severity	Source	Description	Remedial Action
Information	SSL	SSL certificate deleted.	No action required.

SSL disabled

Type/Severity	Source	Description	Remedial Action
Information	SSL	SSL is disabled.	No action required.

SSL enabled

Type/Severity	Source	Description	Remedial Action
Information	SSL	SSL is enabled.	No action required.

SSL server reset

Type/Severity	Source	Description	Remedial Action
Information	SSL	SSL server reset.	No action required.

Comments? infodev@avaya.com

Chapter 58: Stack Manager messages

Stack Manager critical messages

application-name failed DB-exchange stack failed to form

Type/Severity	Source	Description	Remedial Action
Critical	Stack Manager	The stack did not form, as the application <application-name> did not exchange its database successfully.	Reboot the stack.

Stack Manager warning messages

application-name failed DB-exchange stack formation delayed

Type/Severity	Source	Description	Remedial Action
Serious	Stack Manager	The application <application-name> failed to exchange its database.	Reboot the unit if it is unsuccessful in joining the stack.

Base unit has loopback port mode %s and the current unit %s. Unit reconfigured and rebooted

Type/Severity	Source	Description	Remedial Action
Serious	Stack Manager	The loopback port mode of the current unit is different than the BU's. Current unit will reconfigure and will be rebooted. Loopback port modes are: stack, rear, MDA, none.	No action required.

Different spanning-tree mode configured than BU. Unit reconfigured and rebooted.

Type/Severity	Source	Description	Remedial Action
Serious	Stack Manager	Current unit has different spanning-tree mode than the one used by BU. Unit will be reconfigured and rebooted.	No action required.

Front-panel UI selected use rear-panel base non-base switch

Type/Severity	Source	Description	Remedial Action
Serious	Stack Manager	The stack has been reset using the front-panel push-button.	No action required.

Comments? infodev@avaya.com

QOS filter-limiting mode modified and unit reset

Type/Severity	Source	Description	Remedial Action
Serious	Stack Manager	The QOS filter-limiting mode was modified and the unit rebooted.	No action required.

Stack operation mode modified to Hybrid and unit reset

Type/Severity	Source	Description	Remedial Action
Serious	Stack Manager	Operational Mode was automatically changed and unit was restarted.	No action required.

Stack sync failed stack failed to form

Type/Severity	Source	Description	Remedial Action
Serious	Stack Manager	The stack did not form as the stack synchronization failed.	Reboot the stack.

Stack synchronization failed Exp value Act value Missing value

Type/Severity	Source	Description	Remedial Action
Serious	Stack Manager	Stack synchronization failed on the unit. Missing value yields the application(s) that caused failure.	Reboot the unit if it is unsuccessful in joining the stack.

The base (unit# number) has left the stack. Unit# number is now the base

Type/Severity	Source	Description	Remedial Action
Serious	Stack Manager	The Base unit has left the stack, a new unit has replaced it.	Examine the base unit that left the stack.

Wrong QoS Agent queue setting, expected %u, actual %u, unit reconfigured and reboot

Parameters	Type/ Severity	Source	Description	Remedial Action
BU QoS queue set size and unit QoS queue set size	Serious	Stack Manager	Non Bu QoS queue set size is checked at discovery against BU's QoS que set, changed if needed, unit is rebooted if value is changed.	Assure that QoS queue set size on Non Base Units is the same as the BU QoS queue set size.

Wrong QoS Agent buffer setting, expected %s, actual %s, unit re-configured and reboot

Type/Severity	Source	Description	Remedial Action
Serious	STKMGR	QoS agent buffer allocation is different that the one of the BU's.	Wait for re-configuration and reboot cycle.

Comments? infodev@avaya.com

Wrong QoS Agent queue setting, expected %u, actual %u, unit re-configured and reboot

Type/Severity	Source	Description	Remedial Action
Serious	STKMGR	QoS agent queue setting is different that the one of the BU's.	Wait for re-configuration and reboot cycle.

Different spanning-tree mode configured than BU. Unit re-configured and rebooted

Type/Severity	Source	Description	Remedial Action
Serious	STKMGR	Spanning tree mode is different than BU's.	Wait for re-configuration and reboot cycle.

Stack Manager information messages

Another BU tried to join the stack. Unit ignored

Type/Severity	Source	Description	Remedial Action
Information	Stack Manager	A switch having BU switch selected was added to an existing stack.	Unset BU switch from the new added unit.

BECOME_TEMP_BU event sent unit mask value appl mask value

Type/Severity	Source	Description	Remedial Action
Information	Stack Manager	The unit on which this message is logged has	No action required.

Type/Severity	Source	Description	Remedial Action
		become the temporary base unit.	

Change of active config block and or reset failed block-number

Type/Severity	Source	Description	Remedial Action
Information	Stack Manager	Active configuration block was changed and the unit was restarted.	No action required.

DISTRIBUTE_DB event sent unit mask value appl mask value

Type/Severity	Source	Description	Remedial Action
Information	Stack Manager	The DISTRIBUTE_DB event is sent during the stack formation process.	No action required.

Filter limiting mode not supported on 5510-XX unit cannot join stack

Type/Severity	Source	Description	Remedial Action
Information	Stack Manager	Filter limiting mode is different than the base unit's mode. Some modes are not supported in the ERS 55XX..	Modify the Filter Limiting mode on the base unit or remove the ERS 55XX.

JOIN event sent unit mask value appl mask value

Type/Severity	Source	Description	Remedial Action
Information	Stack Manager	The Join event is sent during the stack formation process.	No action required.

Comments? infodev@avaya.com

LEAVE event sent unit mask value appl mask value

Type/Severity	Source	Description	Remedial Action
Information	Stack Manager	The unit on which this message is logged has left the stack. The 'unit mask' is a bit mask representation of the unit that left the stack.	Make sure that the unit removal is intended.

MODULE_INACTIVE event sent unit mask value appl mask value

Type/Severity	Source	Description	Remedial Action
Information	Stack Manager	A unit has left the stack. The 'unit mask' is a bit mask representation of the unit that left the stack.	Make sure that the unit removal is intended.

More than value units discovered

Type/Severity	Source	Description	Remedial Action
Information	Stack Manager	Too many units are in the stack.	Remove the extra unit(s).

Multiple base units detected

Type/Severity	Source	Description	Remedial Action
Information	Stack Manager	The system detected more than one configured base unit.	Reconfigure the extra base unit(s) to non-base units.

Multiple Waverunner units detected when base is a Flagship

Type/Severity	Source	Description	Remedial Action
Information	Stack Manager	Too many ERS56XX units are in stack.	Remove the extra 56XX unit(s) or make 56XX the base unit.

REMOVE_DATA event sent unit mask value appl mask value

Type/Severity	Source	Description	Remedial Action
Information	Stack Manager	The application could not exchange its database successfully.	No action required.

Stack operation mode modified to Pure and unit reset

Type/Severity	Source	Description	Remedial Action
Information	Stack Manager	Operational Mode was automatically changed and unit was restarted.	No action required.

The BU switch is enabled. Cannot join existing stack

Type/Severity	Source	Description	Remedial Action
Information	Stack Manager	The switch has BU switch set and is added to an existing stack.	Unset BU switch before adding it to a new stack.

Comments? infodev@avaya.com

This unit has wrong F W version expected version actual version

Type/Severity	Source	Description	Remedial Action
Information	Stack Manager	The unit did not join the stack because the F/W is different than base unit's F/W .	Download the correct F/W or configure the unit to automatically download it from the base unit.

This unit has wrong S W version expected version actual version

Type/Severity	Source	Description	Remedial Action
Information	Stack Manager	The unit did not join the stack because the S/W is different than the base unit's S/W .	You should download the correct S/W or configure the unit to automatically download it from base unit.

Wrong QOS Agent buffer setting expected value actual value unit cannot join stack.

Type/Severity	Source	Description	Remedial Action
Information	Stack Manager	The QOS buffer setting on this unit is different than that of the base unit's setting.	Modify the QOS buffer setting on the unit.

Stack must have a configured base unit!

Type/Severity	Source	Description	Remedial Action
Information	STKMGR	No Base Unit is configured in the stack.	Configure one Base Unit in the stack.

Replaced "Wrong QoS Agent buffer setting, expected %u, actual %u, unit cannot join stack" with "Wrong QoS Agent buffer setting, expected %s, actual %s, unit cannot join stack"

Type/Severity	Source	Description	Remedial Action
Information	STKMGR	Unit cannot join the stack because of the difference in buffer setting.	Re-configure QoS agent buffer setting to the expected value and power cycle unit.

Comments? infodev@avaya.com

Chapter 59: Stack Monitor messages

Stack Monitor critical messages

Task task-name is suspended

Type/Severity	Source	Description	Remedial Action
Critical	Stack Monitor	One of the tasks running on the device encountered a critical error and was suspended.	No action required.

Task whose index is taskID taskID is suspended

Type/Severity	Source	Description	Remedial Action
Critical	Stack Monitor	One of the tasks running on the device encountered a critical error and was suspended.	No action required.

Stack Monitor information messages

application_name failed DB-exchange stack formation delayed

Type/Severity	Source	Description	Remedial Action
Information	Stack Monitor	The application name in the Stack Monitor failed the DB exchange for three times simultaneously.	No action required. The Stack Manager will wait for 3 minutes after a DB-exchange failure and then restart the stack formation process. The logs are saved to NVRAM for future reference.

Hello Module unable to communicate with neighbor(s) unit reset

Type/Severity	Source	Description	Remedial Action
Information	Stack Monitor	The Hello module is unable to communicate with the neighbor(s), as the stack port direction(s) are logically down for more than 5 minutes.	No action required.The switch/stack reboots itself. The logs are saved to NVRAM for future reference.

IMC buffers of size size have been exhausted buffer pool size size

Type/Severity	Source	Description	Remedial Action
Information	Stack Monitor	Stack Monitor detected a depleted IMC (Inter-Module Communication) buffer pool.	No action required. The switch/stack reboots itself. The logs are saved to NVRAM for future reference.

Comments? infodev@avaya.com

Stack synchronization failed stack formation delayed

Type/Severity	Source	Description	Remedial Action
Information	Stack Monitor	The Stack Manager did not receive an acknowledgement after sending the Join message to all the Non Base units for three times in a row.	No action required. The switch/stack reboots itself. The logs are saved to NVRAM for future reference.

Task whose index is Index1 Index2 is suspended

Type/Severity	Source	Description	Remedial Action
Information	Stack Monitor	Stack Monitor detected that a task has been suspended for more than 5 minutes.	No action required. The switch/stack reboots itself. The logs are saved to NVRAM for future reference.

Task task_name is suspended

Type/Severity	Source	Description	Remedial Action
Information	Stack Monitor	Stack Monitor detected that a task has been suspended for more than 5 minutes.	No action required. The switch/stack reboots itself. The logs are saved to NVRAM for future reference.

The number of stack units is number instead of expected number

Type/Severity	Source	Description	Remedial Action
Information	Stack Monitor	The number of units in the stack differs from the one	Check if any units are down or unresponsive. Also check if the Stack Monitor is

Type/Severity	Source	Description	Remedial Action
		configured in Stack Monitor.	misconfigured (that is the configured number of units is different from the real number of units in stack)

Comments? infodev@avaya.com

Chapter 60: Source Based Routing Messages

Source Based Routing Information Messages

Topic title

Insert a brief overview of the topic to help the user decide whether this reference topic is relevant to them. Briefly describe what the reference item does, what it is, or what it is used for. In most cases, use a complete sentence.. Avoid using the abstract to lead in or build up to a topic. Use complete sentence rather than sentence fragments, and do not simply repeat the title. Avoid starting abstracts with phrases such as "This topic describes . . . ." or "This topic is about . . . ."

IpFwdNhop Err Filter Install mod_inst=0x%08x vid=%d rv=%d

Type/Severity	Source	Description	Remedial Action
Information	Source Based Routing	Error when installing policy based routing filter in hardware.	No action required.

IpFwdNhop Err Filter Modify mod_inst=0x%08x vid=%d rv=%d

Type/Severity	Source	Description	Remedial Action
Information	Source Based Routing	Error when modifying policy based routing filter in hardware.	No action required.

IpFwdNhop Err Filter UnInstall mod_inst=0x%08x vid=%d rv=%d

Type/Severity	Source	Description	Remedial Action
Information	Source Based Routing	Error when uninstalling policy based routing filter in hardware.	No action required.

IpFwdNhop Err Filter UnInstall mod_inst=0x%08x vid=%d rv=%d

Type/Severity	Source	Description	Remedial Action
Information	Source Based Routing	Error when uninstalling policy based routing filter in hardware.	No action required.

IpFwdNhop Err Save DB to NVRAM General File myMod=%d isBU=%d rw=%d

Type/Severity	Source	Description	Remedial Action
Information	Source Based Routing	Error when saving global SBR settings to NVRAM.	No action required.

IpFwdNhop Err Save DB to NVRAM Instance File myMod=%d isBU=%d rw=%d

Type/Severity	Source	Description	Remedial Action
Information	Source Based Routing	Error when saving SBR instances to NVRAM.	No action required.

Comments? infodev@avaya.com

IpFwdNhop Err Save DB to NVRAM Policy File myMod=%d isBU=%d rw=%d

Type/Severity	Source	Description	Remedial Action
Information	Source Based Routing	Error when saving SBR policies to NVRAM.	No action required.

IpFwdNhop: Feature enable temporarily blocked - resources unavailable

Type/Severity	Source	Description	Remedial Action
Information	Source Based Routing	Indicates that the required resources for enabling the SBR feature are not available.	No action required.

IpFwdNhop: Filter installation issue - resources unavailable

Type/Severity	Source	Description	Remedial Action
Information	Source Based Routing	Error when installing policy based routing filter in hardware.	No action required.

IpFwdNhop: Issue detected during data restore (interface entry %d)

Type/Severity	Source	Description	Remedial Action
Information	Source Based Routing	Indicates an error when try to install filters for attached policies after boot.	No action required.

IpFwdNhop: Issue detected during enable retry (interface entry %d)

Type/Severity	Source	Description	Remedial Action
Information	Source Based Routing	Indicates an error when try to install filters for instances missing them.	No action required.

IpFwdNhop: Issue detected during feature enable (interface entry %d)

Type/Severity	Source	Description	Remedial Action
Information	Source Based Routing	Indicates an error when enabling the SBR feature globally (failed installing filter).	No action required.

IpFwdNhop: Issue detected during interface creation (interface entry %d)

Type/Severity	Source	Description	Remedial Action
Information	Source Based Routing	When create interface event is processed, this indicates a failure when installing the filter for SBR policy.	No action required.

Comments? infodev@avaya.com

IpFwdNhop: Issue detected during VLAN %d routing status update

Type/Severity	Source	Description	Remedial Action
Information	Source Based Routing	When ip routing enable (per VLAN interface) event is processed, this Indicates a failure when installing the filter for SBR policy.	No action required.

IpFwdNhop: Issue detected during VLAN membership addition (VID %d)

Type/Severity	Source	Description	Remedial Action
Information	Source Based Routing	Indicates an error when adding a port to an installed ip-fwd policy.	No action required.

IpFwdNhop: Issue detected during VLAN membership deletion (VID %d)

Type/Severity	Source	Description	Remedial Action
Information	Source Based Routing	Indicates an error when deleting a port from an installed ip-fwd policy.	No action required.

IpFwdNhop: Issue detected during VLAN policy association (entry %d)

Type/Severity	Source	Description	Remedial Action
Information	Source Based Routing	Indicates an error when attaching a SBR policy to a VLAN (failed installing filter).	No action required.

IpFwdNhop: Requested precedence and/or filter resources unavailable

Type/Severity	Source	Description	Remedial Action
Information	Source Based Routing	Indicates that no valid precedence values are available.	No action required.

IpFwdNhop: Requested range checking resources unavailable

Type/Severity	Source	Description	Remedial Action
Information	Source Based Routing	Indicates that range check resources are not available.	No action required.

IpFwdNhop: VLAN membership update (VID %d) issue - resources unavailable

Type/Severity	Source	Description	Remedial Action
Information	Source Based Routing	When a VLAN membership update event is processed, this indicates that the	No action required.

Comments? infodev@avaya.com

Type/Severity	Source	Description	Remedial Action
		required resources for port addition are not available.	

Comments? infodev@avaya.com

Chapter 61: TACACS messages

TACACS information messages

TACACS+ accounting disabled

Type/Severity	Source	Description	Remedial Action
Information	TACACS	Command logging (accounting) is disabled.	No action required.

TACACS+ accounting enabled

Type/Severity	Source	Description	Remedial Action
Information	TACACS	Command logging (accounting) is enabled.	No action required.

TACACS authentication on stack serial disabled

Type/Severity	Source	Description	Remedial Action
Information	TACACS	TACACS authentication disabled on stack serial console.	No action required.

TACACS authentication on stack serial enabled

Type/Severity	Source	Description	Remedial Action
Information	TACACS	TACACS authentication enabled on stack serial console.	No action required.

TACACS+ authentication on switch serial port disabled

Type/Severity	Source	Description	Remedial Action
Information	TACACS	TACACS authentication disabled on the switch serial console.	No action required.

TACACS+ authentication on switch serial port enabled

Type/Severity	Source	Description	Remedial Action
Information	TACACS	TACACS authentication enabled on switch serial console.	No action required.

TACACS authentication on stack telnet disabled

Type/Severity	Source	Description	Remedial Action
Information	TACACS	TACACS authentication disabled on stack telnet.	No action required.

Comments? infodev@avaya.com

TACACS authentication on stack telnet enabled

Type/Severity	Source	Description	Remedial Action
Information	TACACS	TACACS authentication enabled on stack telnet.	No action required.

TACACS+ authentication on switch telnet disabled

Type/Severity	Source	Description	Remedial Action
Information	TACACS	TACACS+ authentication is disabled on switch telnet.	No action required.

TACACS+ authentication on switch telnet enabled

Type/Severity	Source	Description	Remedial Action
Information	TACACS	TACACS+ authentication is disabled on switch telnet.	No action required.

TACACS+ authentication on switch telnet disabled

Type/Severity	Source	Description	Remedial Action
Information	TACACS	TACACS authentication disabled on switch telnet.	No action required.

TACACS+ authentication on switch telnet enabled

Type/Severity	Source	Description	Remedial Action
Information	TACACS	TACACS authentication enabled on switch telnet.	No action required.

TACACS+ authenticated serial connection closed

Type/Severity	Source	Description	Remedial Action
Information	TACACS	TACACS authenticated serial console session was closed.	No action required.

TACACS+ authenticated telnet session closed

Type/Severity	Source	Description	Remedial Action
Information	TACACS	Telnet session authenticated through TACACS closed.	No action required.

TACACS+ authenticated telnet session max retries exceeded

Type/Severity	Source	Description	Remedial Action
Information	TACACS	The maximum number of retries for a TACACS authenticated telnet session exceeded.	No action required.

Comments? infodev@avaya.com

TACACS authenticated SSH session closed

Type/Severity	Source	Description	Remedial Action
Information	TACACS	TACACS authenticated SSH session has closed.	No action required.

TACACS+ authorization disabled

Type/Severity	Source	Description	Remedial Action
Information	TACACS	Command authorization is disabled.	No action required.

TACACS+ authorization enabled

Type/Severity	Source	Description	Remedial Action
Information	TACACS	Command authorization is enabled.	No action required.

TACACS+ unsuccessful authentication

Type/Severity	Source	Description	Remedial Action
Information	TACACS	User authentication failed.	No action required.

TACACS+ successful authentication

Type/Severity	Source	Description	Remedial Action
Information	TACACS	User authentication succeeded.	No action required.

Comments? infodev@avaya.com

Chapter 62: Telnet messages

Telnet information messages

Connection closed. Maximum number of sessions reached. IP address:

Parameters	Type/ Severity	Source	Description	Remedial Action
IP Address	Information	Telnet Server	Telnet server has reached its maximum connections. No new connections currently allowed.	Disconnect at least one telnet connection.

CLI pswd: Stack auth type RADIUS/TACACS+ won't apply partially (stack IP addr not set). Local user/pass used

Type/Severity	Source	Description	Remedial Action
Information	Telnet	Stack IP address is not set	No action required.

CLI pswd: Stack auth type RADIUS/TACACS+ won't apply partially (switch IP addr not set). Local user/pass used

Type/Severity	Source	Description	Remedial Action
Information	Telnet	Switch IP address is not set	No action required.

Successful telnet connection to IP address

Type/Severity	Source	Description	Remedial Action
Information	Telnet	Successful telnet connection.	No action required.

Telnet session closed by ip address remote host.

Type/Severity	Source	Description	Remedial Action
Information	Telnet	Remote host closed the telnet session.	No action required.

TELNET: Telnet connection to IP ip address was closed because parent console session console session ID was closed.

Type/Severity	Source	Description	Remedial Action
Information	Telnet	Telnet Connection was closed because the console session - from which Telnet was launched - was closed..	No action required.

Connection closed. Maximum number of sessions reached. IP address:

Type/Severity	Source	Description	Remedial Action
Information	Telnet server	The maximum number of active telnet connections has been reached.	Close other active sessions in order to free Telnet server slots.

Comments? infodev@avaya.com

Local authentication enabled on serial

Type/Severity	Source	Description	Remedial Action
Information	CLI	Authentication on serial port using local credentials has been enabled.	No action required.

Local authentication disabled on serial

Type/Severity	Source	Description	Remedial Action
Information	CLI	Authentication on serial port using local credentials has been disabled.	No action required.

Local authentication enabled on telnet

Type/Severity	Source	Description	Remedial Action
Information	CLI	Authentication over telnet using local credentials has been enabled.	No action required.

Local authentication disabled on telnet

Type/Severity	Source	Description	Remedial Action
Information	CLI	Authentication over telnet using local credentials has been disabled.	No action required.

Session opened (local auth) from IP address:

Type/Severity	Source	Description	Remedial Action
Information	Telnet server	Successful authentication with local credentials over telnet session.	No action required.

Failed login (local auth) from IP address:

Type/Severity	Source	Description	Remedial Action
Information	Telnet server	Failed authentication with local credentials over telnet session.	Enter correct local username and password.

Session opened (local auth) from serial connection

Type/Severity	Source	Description	Remedial Action
Information	Console	Successful authentication with local credentials on serial port.	No action required.

Failed login (local auth) from serial connection

Type/Severity	Source	Description	Remedial Action
Information	Console	Failed authentication with local credentials on serial port.	Enter correct local username and password.

Comments? infodev@avaya.com

Chapter 63: USB messages

USB information messages

USB device inserted

Type/Severity	Source	Description	Remedial Action
Information	USB	A USB memory stick has been inserted in the unit.	No action required.

USB device removed

Type/Severity	Source	Description	Remedial Action
Information	USB	A USB memory stick has been removed from the unit.	No action required.

Comments? infodev@avaya.com

Chapter 64: Telnet Server messages

Telnet Server warning messages

Reset initiated by console

Type/Severity	Source	Description	Remedial Action
Serious	Console	Reset is initiated through a serial connection.	No action required.

Reset initiated through SSH by IP address

Type/Severity	Source	Description	Remedial Action
Serious	Telnet Server	Reset initiated through the SSH connection.	No action required.

Reset initiated through telnet by IP address

Type/Severity	Source	Description	Remedial Action
Serious	Telnet Server	Reset is initiated through a telnet connection.	No action required.

Reset to default initiated by console

Type/Severity	Source	Description	Remedial Action
Serious	Console	Reset to the default settings initiated through serial connection.	No action required.

Reset to default initiated through telnet by IP address

Type/Severity	Source	Description	Remedial Action
Serious	Telnet Server	Reset to default settings initiated through the telnet connection.	No action required.

Stack RO password changed from IP add

Type/Severity	Source	Description	Remedial Action
Serious	Telnet Server	Stack RO (Read Only) password changed from telnet or SSH session.	No action required.

Stack RO password changed from serial conn

Type/ Severity	Source	Description	Remedial Action
Serious	Console	Stack RO (Read Only) password changed from the serial connection session.	No action required.

Comments? infodev@avaya.com

Stack RW password changed from IP add

Type/Severity	Source	Description	Remedial Action
Serious	Telnet Server	Stack RW (Read Write) password changed from telnet or SSH session.	No action required.

Stack RW password changed from serial conn

Type/Severity	Source	Description	Remedial Action
Serious	Console	Stack RW (Read Write) password changed from the serial connection session.	No action required.

Switch RO password changed from IP add

Type/Severity	Source	Description	Remedial Action
Serious	Telnet Server	Switch RO (Read Only) password changed from telnet or SSH session.	No action required.

Switch RO password changed from serial conn

Type/Severity	Source	Description	Remedial Action
Serious	Console	Switch RO (read-only) password changed from the serial connection session.	No action required.

Switch RW password changed from IP add

Type/Severity	Source	Description	Remedial Action
Serious	Telnet Server	Switch RW (Read Write) password changed from the telnet or the SSH session.	No action required.

Switch RW password changed from serial conn

Type/Severity	Source	Description	Remedial Action
Serious	Console	Switch RW (Read Write) password changed from the serial connection session.	No action required.

Telnet Server information messages

Connection closed (failed login) IP address

Type/Severity	Source	Description	Remedial Action
Information	Telnet Server	The connection was disconnected after three login attempts failed.	Enter a valid username and password.

Comments? infodev@avaya.com

Connection closed (inactivity logout) IP address

Type/Severity	Source	Description	Remedial Action
Information	Telnet Server	Client was disconnected by the server after 15 minutes of terminal inactivity.	No action required.

Connection closed (login timeout) IP address

Type/Severity	Source	Description	Remedial Action
Information	Telnet Server	The Telnet Login prompt message is available for the user input for one minute with maximum of three attempts. If you do not provide a valid username and password the connection will be disconnected.	Enter the correct username and password within one minute.

Connection closed (lost connection) IP address

Type/Severity	Source	Description	Remedial Action
Information	Telnet Server	Client aborted the connection (RST message is sent).	No action required.

Connection closed (user logout) IP address

Type/Severity	Source	Description	Remedial Action
Information	Telnet Server	User ends telnet session. The connection is lost.	No action required.

Disallowed connection attempt from IP address

Type/Severity	Source	Description	Remedial Action
Information	Telnet Server	Telnet-access is disabled or the client IP address does not pass the telnet-access/IP manager rules. Hence, the client connection is dropped.	Check the telnet-access/IP manager configuration and modify the settings accordingly.

Disallowed connection attempt - too many telnet sessions

Type/Severity	Source	Description	Remedial Action
Information	Telnet Server	The attempt to telnet session connection is disallowed, as the maximum number of telnet sessions is reached.	No action required.

Failed login from IP address

Type/Severity	Source	Description	Remedial Action
Information	Telnet Server	You have entered an incorrect username or password.	Enter a valid username and password.

Failed login from serial connection

Type/Severity	Source	Description	Remedial Action
Information	Console	You have entered an incorrect username or password on the serial interface.	Enter a valid username and password.

Comments? infodev@avaya.com

Failed login(radius auth) from IP add

Type/Severity	Source	Description	Remedial Action
Information	Telnet Server	You have failed to login as the Radius Server authentication is required for the telnet connections.	Enter a valid username and password.

Failed login(radius auth) from serial conn

Type/ Severity	Source	Description	Remedial Action
Console	Telnet Server	You failed to login as the Radius Server authentication is required for serial connections.	Enter a valid username and password.

Login timeout serial connection

Type/Severity	Source	Description	Remedial Action
Information	Console	The serial connection login prompt message is available for the user input for one minute with maximum of three attempts, if you fail to login the product banner is displayed.	Enter a valid username and password within a minute.

Session closed (inactivity logout) IP address

Type/Severity	Source	Description	Remedial Action
Information	Telnet Server	The telnet session is disconnected after 15	No action required.

Type/Severity	Source	Description	Remedial Action
		minutes of console inactivity.	

Session closed (inactivity logout) IP address

Type/Severity	Source	Description	Remedial Action
Information	Telnet Server	Telnet session was disconnected after 15 minutes of console inactivity.	No action required.

Session closed (lost connection) IP address

Type/Severity	Source	Description	Remedial Action
Information	Telnet Server	Client aborted the connection by sending a RST message. The server disconnected the session.	No action required.

Session closed (user logout) IP address

Type/Severity	Source	Description	Remedial Action
Information	Telnet Server	You have disconnected the telnet session.	No action required.

Session closed (user logout) serial connection

Type/Severity	Source	Description	Remedial Action
Information	Console	You have disconnected the serial connection session.	No action required.

Comments? infodev@avaya.com

Session opened from IP address

Type/Severity	Source	Description	Remedial Action
Information	Telnet Server	The telnet session has begun. You now have the access to the terminal using the CTRL-Y key or you have successfully logged-in, in case of authentication requirement.	No action required.

Session opened from serial connection

Type/Severity	Source	Description	Remedial Action
Information	Console	Session has begun on the serial connection. You now have access to the terminal using the CTRL-Y key or successfully logged-in, in the case of authentication requirement.	No action required.

Session opened(radius auth) from IP add

Type/Severity	Source	Description	Remedial Action
Information	Telnet Server	You have successfully logged in with the Radius Server. Telnet session has begun.	No action required.

Session opened(radius auth) from serial conn

Type/Severity	Source	Description	Remedial Action
Information	Console	You have successfully logged-in with the Radius	No action required.

Type/Severity	Source	Description	Remedial Action
		Server. The serial connection session is opened.	

Successful connection from IP address

Type/Severity	Source	Description	Remedial Action
Information	Telnet Server	The client is successfully connected to the telnet server.	No action required.

Comments? infodev@avaya.com

Chapter 65: Unicast Storm Control messages

Unicast Storm Control information messages

Unicast unblock unit port unit_port level level watermark watermark

Type/Severity	Source	Description	Remedial Action
Information	port driver	Unicast blocking is disabled on the indicated port as it reached below the high water mark level.	No action required.

Unicast block unit port unit_port level level watermark watermark

Type/Severity	Source	Description	Remedial Action
Information	port driver	Unicast blocking is enabled on the indicated port as it reached the high water mark level.	Investigate the cause of the unicast storm to ensure optimal network performance.

USC Install SET fail unit port unit_port status = status

Type/Severity	Source	Description	Remedial Action
Information	port driver	Installation of the Unicast Storm Control filter during set phase failed for the indicated port.	Verify that the hardware filter resources are available for the indicated port. Current hardware filter resource

Type/Severity	Source	Description	Remedial Action
			usage can be displayed through the 'show qos diag' command. You may need to disable other applications currently using hardware filter resources in order to free them up for the Unicast Storm Control application.

USC Install TEST fail unit port unit_port status = status

Type/Severity	Source	Description	Remedial Action
Information	port driver	Installation of the Unicast Storm Control filter during test phase failed for the indicated port.	Verify the hardware filter resources are available for the indicated port. Current hardware filter resource usage can be displayed through the 'show qos diag' command. You may need to disable other applications currently using hardware filter resources in order to free them up for the Unicast Storm Control application.

USC UnInst SET failed for port port status = status

Type/Severity	Source	Description	Remedial Action
Information	port driver	The Unicast Storm Control filter could not be uninstalled during the set phase for the indicated port.	Verify the hardware filter resources have been un-installed for the Unicast Storm Control application. If not, reboot it to successfully remove any hardware filter resources that are still attached to the Unicast Storm Control application.

Comments? infodev@avaya.com

Chapter 66: VLACP messages

VLACP information messages

Port %d blocked by VLACP until end-partner connection reestablished

Parameters	Type/Severity	Source	Description	Remedial Action
Unit /Port	Information	VLACP	Blocking port due to not receiving VLACP packages from partner.	Check links between units or settings.

Port %d reenabled by VLACP

Parameters	Type/Severity	Source	Description	Remedial Action
Unit /Port	Information	VLACP	VLACP message received from partner, re-enabling.	No action required.

Port unit# port# blocked by VLACP until end-partner connection reestablished

Type/Severity	Source	Description	Remedial Action
Information	VLACP	Port put to Listening by VLACP.	No action required.

Port unit# port# reenabled by VLACP

Type/Severity	Source	Description	Remedial Action
Information	VLACP	Port put back to its state by VLACP.	No action required.

Comments? infodev@avaya.com

Chapter 67: VLAN messages

VLAN information messages

BU was unable to send IMC for NBUs VLAN/Port configuration

Type/Severity	Source	Description	Remedial Action
Information	VLAN	There was an error when sending VLAN configuration to stack.	No action required.

Cli add vlan vlan id members port mask

Type/Severity	Source	Description	Remedial Action
Information	VLAN	Add new members indicated in port list to VLAN.	No action required.

Cli create vlan vlan id type port

Type/Severity	Source	Description	Remedial Action
Information	VLAN	A new VLAN type port is created.	No action required.

Cli delete vlan vlan id members port mask

Type/Severity	Source	Description	Remedial Action
Information	VLAN	Remove members indicated in port list from VLAN.	No action required.

Cli delete vlan vlan id type port

Type/Severity	Source	Description	Remedial Action
Information	VLAN	The existing VLAN type port is deleted.	No action required.

Cli set autopvid disable

Type/Severity	Source	Description	Remedial Action
Information	VLAN	Disable the auto PVID.	No action required.

Cli set autopvid enable

Type/Severity	Source	Description	Remedial Action
Information	VLAN	Enable auto PVID.	No action required.

Cli set management vlan vlan id

Type/Severity	Source	Description	Remedial Action
Information	VLAN	Set the management VLAN.	No action required.

Comments? infodev@avaya.com

Cli set ports port mask tagging disable

Type/Severity	Source	Description	Remedial Action
Information	VLAN	Port tagging is disabled.	No action required.

Cli set ports port mask tagging enable

Type/Severity	Source	Description	Remedial Action
Information	VLAN	Port tagging is enabled.	No action required.

Cli set pvid vlan id ports port mask

Type/ Severity	Source	Description	Remedial Action
Information	VLAN	Port PVID is set.	No action required.

Cli set vlan vlan id members port mask

Type/Severity	Source	Description	Remedial Action
Information	VLAN	VLAN ports are set.	No action required.

Cons activate vlan vlan id

Type/Severity	Source	Description	Remedial Action
Information	VLAN	VLAN is activated.	No action required.

Cons add vlan vlan id port unit port

Type/Severity	Source	Description	Remedial Action
Information	VLAN	Port is added to VLAN.	No action required.

Cons create vlan vlan id type port

Type/Severity	Source	Description	Remedial Action
Information	VLAN	New VLAN type port is created.	No action required.

Cons delete vlan vlan id port unit port

Type/ Severity	Source	Description	Remedial Action
Information	VLAN	Port is removed from VLAN.	No action required.

Cons delete vlan vlan id type port

Type/Severity	Source	Description	Remedial Action
Information	VLAN	Existing VLAN type port is deleted.	No action required.

Cons set autopvid disable

Type/Severity	Source	Description	Remedial Action
Information	VLAN	Disable auto PVID.	No action required.

Comments? infodev@avaya.com

Cons set autopvid enable

Type/Severity	Source	Description	Remedial Action
Information	VLAN	Enable auto PVID.	No action required.

Cons set management vlan vlan id

Type/Severity	Source	Description	Remedial Action
Information	VLAN	Management VLAN is set.	No action required.

Cons set port unit port pvid vlan id

Type/Severity	Source	Description	Remedial Action
Information	VLAN	Port PVID is set.	No action required.

Cons set port unit port tagging disable

Type/Severity	Source	Description	Remedial Action
Information	VLAN	Port tagging is disabled.	No action required.

Cons set port unit port tagging enable

Type/Severity	Source	Description	Remedial Action
Information	VLAN	Port tagging enabled.	No action required.

Error getting VLAN info for Port's pvid

Type/Severity	Source	Description	Remedial Action
Information	VLAN	There was an error when reading the VLAN configuration from NVRAM.	No action required.

Error reading nvq_ObjDescr from VLAN file

Type/Severity	Source	Description	Remedial Action
Information	VLAN	There was an error when reading the VLAN configuration from NVRAM.	No action required.

Error reading prec from VLAN file

Type/Severity	Source	Description	Remedial Action
Information	VLAN	There was an error when reading the VLAN configuration from NVRAM.	No action required.

Error reading vmrec from VLAN file

Type/Severity	Source	Description	Remedial Action
Information	VLAN	There was an error when reading the VLAN configuration from NVRAM.	No action required.

Comments? infodev@avaya.com

Error reading vrec from VLAN file

Type/Severity	Source	Description	Remedial Action
Information	VLAN	There was an error when reading the VLAN configuration from NVRAM.	No action required.

Error restoring Ports from VLAN file

Type/Severity	Source	Description	Remedial Action
Information	VLAN	There was an error when reading the VLAN configuration from NVRAM.	No action required.

Error restoring Port from VLAN NVRAM file

Type/Severity	Source	Description	Remedial Action
Information	VLAN	There was an error when reading the VLAN configuration from NVRAM.	No action required.

Error restoring from VLAN file

Type/Severity	Source	Description	Remedial Action
Information	VLAN	There was an error when reading the VLAN configuration from NVRAM.	No action required.

Error restoring from VLAN file. Wrong nvq.Descr.devVer

Type/Severity	Source	Description	Remedial Action
Information	VLAN	There was an error when reading the VLAN configuration from NVRAM.	No action required.

Error restoring from VLAN file. Wrong nvq.Descr.notBlank

Type/Severity	Source	Description	Remedial Action
Information	VLAN	There was an error when reading the VLAN configuration from NVRAM.	No action required.

Error restoring nvq.Descr from VLAN file

Type/Severity	Source	Description	Remedial Action
Information	VLAN	There was an error when reading the VLAN configuration from NVRAM.	No action required.

Error restoring object from VLAN file - bad file pointer or mode

Type/Severity	Source	Description	Remedial Action
Information	VLAN	There was an error when reading the VLAN configuration from NVRAM.	No action required.

Comments? infodev@avaya.com

Error restoring object from VLAN NVRAM file

Type/Severity	Source	Description	Remedial Action
Information	VLAN	There was an error when reading the VLAN configuration from NVRAM.	No action required.

Error seeking object in VLAN file

Type/Severity	Source	Description	Remedial Action
Information	VLAN	There was an error when reading the VLAN configuration from NVRAM.	No action required.

Error restoring VLANs from VLAN file

Type/Severity	Source	Description	Remedial Action
Information	VLAN	There was an error when reading the VLAN configuration from NVRAM.	No action required.

Error restoring VMACs from VLAN file

Type/Severity	Source	Description	Remedial Action
Information	VLAN	There was an error when reading the VLAN configuration from NVRAM.	No action required.

Error seeking Ports in VLAN file

Type/Severity	Source	Description	Remedial Action
Information	VLAN	There was an error when reading the VLAN configuration from NVRAM.	No action required.

Error seeking VLANs in VLAN file

Type/Severity	Source	Description	Remedial Action
Information	VLAN	There was an error when reading the VLAN configuration from NVRAM.	No action required.

Error seeking VMACs in VLAN file

Type/Severity	Source	Description	Remedial Action
Information	VLAN	There was an error when reading the VLAN configuration from NVRAM.	No action required.

Number of VLANs does not match BU number of VLANs. VLAN config defaulted

Type/Severity	Source	Description	Remedial Action
Information	VLAN	VLAN configuration was defaulted because the current number of VLANs does not match the	No action required.

Comments? infodev@avaya.com

Type/Severity	Source	Description	Remedial Action
		Base Unit number of VLANs.	

Set port to default

Type/Severity	Source	Description	Remedial Action
Information	VLAN	There was an error when reading the VLAN configuration from NVRAM.	No action required.

VLAN configuration does not match BU VLAN configuration. VLAN config defaulted

Type/Severity	Source	Description	Remedial Action
Information	VLAN	VLAN configuration was defaulted because the current VLAN configuration does not match the Base Unit VLAN configuration.	No action required.

VLAN IMC callback failed

Type/Severity	Source	Description	Remedial Action
Information	VLAN	There was an error when sending VLAN configuration to stack.	No action required.

VLAN IMC was not sent

Type/Severity	Source	Description	Remedial Action
Information	VLAN	There was an error when sending VLAN configuration to stack.	No action required.

VLAN NVRAM read error

Type/Severity	Source	Description	Remedial Action
Information	VLAN	There was an error when reading the VLAN configuration from NVRAM.	No action required.

VLAN queue messages discarded

Type/Severity	Source	Description	Remedial Action
Information	VLAN	Internal VLAN messages were discarded.	No action required.

Number of VLANs does not match BU number of VLANs. VLAN config defaulted

Type/Severity	Source	Description	Remedial Action
Information	VLAN	The Non-Base Unit has a different number of VLANs than the Base Unit at dbexchange point.	Reconfigure the port settings for this Non-Base Unit.

Comments? infodev@avaya.com

VLAN configuration does not match BU VLAN configuration. VLAN config defaulted

Type/Severity	Source	Description	Remedial Action
Information	VLAN	This Non-Base Unit has the same number of VLANs as the Base Unit, but it has a different VLAN configuration than the Base Unit at dbexchange point.	Reconfigure the port settings for this Non-Base Unit.

VLAN NVRAM read error

Type/Severity	Source	Description	Remedial Action
Information	VLAN	Error at NVRAM restore.	Reconfigure VLAN settings and/or port configuration on this unit.

VLAN set error from IMC

Type/Severity	Source	Description	Remedial Action
Information	VLAN	BU sends IMC to all NBUs and an error occurs when applying Vlan configuration on a NBU.	No action required.

VLAN set error from RPC

Type/Severity	Source	Description	Remedial Action
Information	VLAN	NBU sends RPC to BU and an error	No action required.

Type/Severity	Source	Description	Remedial Action
		occurs when applying Vlan configuration on BU.	

VLAN queue messages discarded

Type/Severity	Source	Description	Remedial Action
Information	VLAN	Logged for each message that was not successfully sent to the VLAN queue.	No action required.

Wrong VLANs nvq_RecDescr actRecs

Type/Severity	Source	Description	Remedial Action
Information	VLAN	There was an error when reading the VLAN configuration from NVRAM.	No action required.

Wrong VMACs nvq_RecDescr actRecs

Type/Severity	Source	Description	Remedial Action
Information	VLAN	There was an error when reading the VLAN configuration from NVRAM.	No action required.

Wrong vrec field

Type/Severity	Source	Description	Remedial Action
Information	VLAN	There was an error when reading the	No action required.

Comments? infodev@avaya.com

Type/Severity	Source	Description	Remedial Action
		VLAN configuration from NVRAM.	

Comments? infodev@avaya.com

Chapter 68: VRRP messages

VRRP information messages

VRRP: vrrpAdvtQueue is FULL. RX advertisement dropped in vlan %d!

Parameters	Type/Severity	Source	Description	Remedial Action
VLAN number	Information	VRRP	vrrpAdvtQueue is FULL.	No action required.

VRRP: vrrpQueue is FULL. Message dropped.

Type/Severity	Source	Description	Remedial Action
Information	VRRP	vrrpQueue is FULL.	No action required.

VRRP Feature globally disabled due to missing license

Type/Severity	Source	Description	Remedial Action
Information	VRRP	Disable the Global VRRP because the license is missing or expired. VRRP will be disabled till the license is installed.	Install a valid Layer3/VRRP license.

VRRP VR VR Id VLAN Id Received mismatching advertisement interval (advertisement interval)

Type/Severity	Source	Description	Remedial Action
Information	VRRP	The system Received a VRRP packet with different advertisement interval. VRRP advertisements from VRRP routers with different advertisement interval will be dropped until problem is solved.	Use or set the same advertisement interval for the VRRP routers.

VRRP VR VR Id VLAN Id Received mismatching advertisement type (advertisement type)

Type/Severity	Source	Description	Remedial Action
Information	VRRP	The system received a VRRP packet with different advertisement type. VRRP advertisements from VRRP routers with different advertisement type will be dropped till the problem is solved.	Use or set the same advertisement type for VRRP routers. Fast advertisement should be either enabled or disabled on all VRRP routers.

VRRP VR VR Id VLAN Id Received mismatching fast advertisement interval (fast advertisement interval)

Type/Severity	Source	Description	Remedial Action
Information	VRRP	The system received a VRRP packet with different fast advertisement interval. VRRP advertisements from VRRP routers with different fast advertisement interval	Use or set the same fast advertisement interval for all VRRP routers.

Comments? infodev@avaya.com

Type/Severity	Source	Description	Remedial Action
		will be dropped till the problem is solved.	

VRRP VR VR Id VLAN Id Received mismatching virtual IP address (received virtual ip address)

Type/Severity	Source	Description	Remedial Action
Information	VRRP	The system received a VRRP packet with different virtual IP address VRRP advertisements from VRRP routers with different virtual IP address will be dropped until problem is solved.	Use or set the same virtual IP address for all VRRP routers.

VRRP VR VR Id VLAN Id Received unknown VRRP packet type (vrrp packet type)

Type/Severity	Source	Description	Remedial Action
Information	VRRP	Received unknown or wrong VRRP packet type. VRRP advertisements from VRRP routers with different VRRP type will be dropped till the problem is solved.	Use or set the same VRRP type for all VRRP routers.

Comments? infodev@avaya.com

Chapter 69: WEB messages

WEB information messages

User allowed (radius authentication pass) to log in from Web from Src IP

Type/Severity	Source	Description	Remedial Action
Information	WEB	Client from the indicated IP address has been authenticated successfully through the Radius server.	No action required.

User disallowed (radius authentication fail) to log in from Web from Src IP

Type/Severity	Source	Description	Remedial Action
Information	WEB	Client from the indicated IP address has failed authentication through the Radius server.	Provide the correct username and password to gain access.

Web authentication fail from IP address

Type/Severity	Source	Description	Remedial Action
Information	WEB	Client from the indicated IP address has failed authentication.	Provide the correct username and password to gain access to the web server.

Web authentication from IP address

Type/Severity	Source	Description	Remedial Action
Information	WEB	Client from the indicated IP address has been successfully authenticated.	No action required.

Web connection from IP address

Type/Severity	Source	Description	Remedial Action
Information	WEB	New client from the indicated IP address is connected to the web server.	No action required.

Web disconnect from IP address

Type/Severity	Source	Description	Remedial Action
Information	WEB	Client from the indicated IP address is disconnected from the web server.	No action required.

Web server attempting to open socket for port HTTP port

Type/Severity	Source	Description	Remedial Action
Information	WEB	Web server is attempting to change communication to the new HTTP port indicated.	No action required.

Comments? infodev@avaya.com

Web server starts service on port HTTP port

Type/Severity	Source	Description	Remedial Action
Information	WEB	Web server is up and running, communicating through the indicated HTTP port.	No action required.

Web timeout from IP address

Type/Severity	Source	Description	Remedial Action
Information	WEB	Client from the indicated IP address has timed out from the web server due to inactivity.	Client may need to login again to gain access to the web server.

Comments? infodev@avaya.com