


ExtremeXOS Installation and Release Notes

Software Version XOS 11.6.3.5

Extreme Networks, Inc.
3585 Monroe Street
Santa Clara, California 95051
(888) 257-3000
(408) 579-2800
<http://www.extremenetworks.com>

Published: September 2007
Part Number: 120334-00 Rev 23



AccessAdapt, Alpine, BlackDiamond, EPICenter, ESRP, Ethernet Everywhere, Extreme Enabled, Extreme Ethernet Everywhere, Extreme Networks, Extreme Standby Router Protocol, Extreme Turbodriven, Extreme Velocity, ExtremeWare, ExtremeWorks, ExtremeXOS, the Go Purple Extreme Solution, ScreenPlay, Sentiariant, ServiceWatch, Summit, SummitStack, Unified Access Architecture, Unified Access RF Manager, UniStack, UniStack Stacking, the Extreme Networks logo, the Alpine logo, the BlackDiamond logo, the Extreme Turbodriven logo, the Summit logos, the Powered by ExtremeXOS logo, and the Color Purple, among others, are trademarks or registered trademarks of Extreme Networks, Inc. or its subsidiaries in the United States and/or other countries.

Adobe, Flash, and Macromedia are registered trademarks of Adobe Systems Incorporated in the U.S. and/or other countries. AutoCell is a trademark of AutoCell. Avaya is a trademark of Avaya, Inc. Merit is a registered trademark of Merit Network, Inc. Internet Explorer is a registered trademark of Microsoft Corporation. Mozilla Firefox is a registered trademark of the Mozilla Foundation. sFlow is a registered trademark of sFlow.org. Solaris and Java are trademarks of Sun Microsystems, Inc. in the U.S. and other countries.

Specifications are subject to change without notice.

All other registered trademarks, trademarks, and service marks are property of their respective owners.

© 2007 Extreme Networks, Inc. All Rights Reserved.

Contents

Chapter 1: Overview	13
New Features in ExtremeXOS 11.6	13
Lab Supported Features in ExtremeXOS 11.6	16
QoS Monitor on BlackDiamond 8800 a-series and e-series Modules, and Summit X450a and X450e Series	16
Supported Hardware	17
BlackDiamond 10808 Component Support	17
BlackDiamond 8810 and BlackDiamond 8806 Component Support	17
BlackDiamond 12804 (R-Series) Component Support	18
Summit X450 Component Support	19
GBIC Support	19
XENPAK Module Support	20
XFP Module Support	22
Chapter 2: Upgrading to ExtremeXOS 11.6	23
Staying Current	23
Upgrading ExtremeXOS	23
Quick Summary	24
Detailed Steps	24
Upgrading ExtremeXOS on a Summit X450	28
Upgrading the BlackDiamond Series of Switches Using Hitless Upgrade	29
Upgrading the Active Partition Using Hitless Upgrade	29
Upgrading the Alternate Partition Using Hitless Upgrade	31
Dual MSM Systems with Different Images Present	32
Using a Rev 10 (or later) BlackDiamond 10808 MSM-1 or MSM-1XL	33
Installing an ExtremeXOS Module	33
Uninstalling an SSH Module	35
Downgrading Switches	35
Chapter 3: Limits	37
Supported Limits	37
Chapter 4: Clarifications and Known Behaviors	47
Clarifications and Known Behaviors	47
General	47
UPM Profiles may take a Long Time to Execute	47
Do not use the “configure sys-recovery-level none” Command	47
Do Not Configure Conflicting System Recovery Levels	47
10 Gigabit Port Shows Local Fault and Link Down in Syslog When Rebooting	48
Process is Lost if Configuration Saved After Terminating Process	48
Saving an SSL Configuration	48
BlackDiamond 8800 Series of Switches	48
Disable RIP Commands Sometimes Causes CLI to Hang	48
“configure vlan protocol ipv6” Command Does not Display	48
Hot Swapping an I/O Module Allows Link Peer to Get an Active Link State	48

RX Over Counter is not Incremented on a BlackDiamond 8800 Switch	48
Conduit Receive Error May Occur on MSM Failover	48
OSPFv3 Can Lose Adjacencies with IPv6 traffic	49
Removing the Primary MSM to Initiate Failover Causes Module is Removed Messages to Appear in the Log.....	49
Hitless Upgrade not Supported	49
When Routing, Ingress Mirrored Traffic is Modified for Routing.....	49
Delay in Displaying FDB Entries.....	49
Untagged VLAN Should Drop Packets.....	49
BlackDiamond 10808 Switch.....	49
BlackDiamond Using 64 ESRP Domains/512 VLANs Generates HAL Core	49
System Health Check Parity Walk Verification Function Should be Enabled.....	50
Output for the "show platform ipv4mc group <group address>" Command Contains an "invalid" Entry	50
BlackDiamond 10808 Crashes with G60T Module.....	50
I/O Modules Fail Due to a Conduit Ping Timeout	50
Incorrect Warning in the Log About the MSM Type	50
BlackDiamond 10808 May Reboot When All PSUs Experience a Brownout	50
Dual Speed 100FX/1000LX SFP Lights When Inserted Without a Link	51
Intel LR XENPAK Module is not Displaying Correctly	51
Opnext ZR XENPAK Module is not Displaying Correctly	51
Intel ER and Intel LR XENPAK Modules are not Displaying Correctly.....	51
Shared Portion of the (TCAM) Memory Blocks Cannot be Reclaimed.....	51
Hot Swapping the Master MSM.....	51
Overflowed Routes and Entries are not Installed Automatically.....	51
BlackDiamond 12800 Series Switches.....	51
MSM B is taking too Long to Come Up	51
Disabling and Enabling a Port Can Take 30 Seconds for Port to Activate	52
I/O Modules take too Much Time to Become Operational	52
ESRP Master Change from BlackDiamond 12804 to BlackDiamond 8800.....	52
Packet Loss Occurs When A BlackDiamond 12804 Becomes ESRP Master.....	52
Downloading an Image Generates Errors in Log	52
BlackDiamond 12804R Enables All Ports at Initial Bootup	52
Backplane Link to Backup MSM Message is not Correct.....	52
"show version" Command May Display Old Firmware Versions	53
Summit Family of Switches.....	53
Summit Switch Logs a Link Down Event with Local Fault	53
Shared Port Link Comes up Before the Software is Initialized	53
On Rebooting SummitX450-24x, Neighboring Switches may see a Link Flap	53
Disabling and Enabling a 100FX Module Displays Wrong Speed	54
Port Number Display is Misleading in Messages	54
L3 Algorithm Flags can be Ignored in the "show ports sharing" Command Output	54
Clearing the System Recovery Level Generates Erroneous Log Messages	54
Management Port Reported as Down in the Shutdown State	54
Reconfiguring the vMAN Ethernet Type is not Effective Until Shared Port is Deleted and Added	54
Load-Sharing Port Removed from STP Domain Without Warning	55
"Slot" Should not be Included in "show inline-power stats" Command Output.....	55
Priority Column Should not be Included in "show inline-power configuration" Command Output	55
"save configuration" Command Must be Performed After Setting Sys-Health-Recovery Level to Shutdown.....	55
"show log" Command Output Filled with sFlow Receiver Missing Message	55
Dot1p-Based QoS Mapping Priority Error	55

Redundant Ports not Correctly Moving to Other Ports in Load Sharing Mode.....	55
“restart ports” Command Runs Too Quickly on a Summit X450	56
Flow Control is Always Reported for 1000 Mbps Link Speed.....	56
Configuration Port Auto-Polarity	56
ACL	56
Default Egress Deny-All ACL Does not Block Multicast Traffic.....	56
ACL Cannot Deny vMAN Traffic with Unknown Destination Address.....	56
Creating Dynamic ACLs Using Operands Results in an Error	56
Summit X450a and Summit X450e series switches and BlackDiamond 8800 a-series and e-series Modules: Boot Time and Timing for Applying ACLs.....	56
Adding Large Number of Dynamic ACLs as Priority First May Fail.....	57
Only One Egress ACL per vMAN Currently Supported	57
Changing the Name of a Rule but not its Conditions or Actions Causes an Error	57
ACL Action replace-dscp Not Taking Effect when Traffic Egresses on a Second Switch	57
ACL actions mirror-cpu and log/log-raw not logging messages	58
Policy-Based Redirect Cannot Redirect Across Two Virtual Routers.....	58
ACL Ethernet SNAP Packets Cause the Wrong Dynamic ACL Counters to Increment.....	58
ACL ICMP Keyword for Timestamp is not Working	58
Modifying a Port Range in an ACL Rule May Cause an ACL Blackhole	58
Cannot Save Policy File Using a Different Name	58
MAC and IP MAC Entries Allowed in the Same IPv6 ACL Rule Entry	58
Invalid Encapsulate Value for IPv6	58
ACL mirror-cpu and log Feature	58
Peer IP Address is Missing in BGP Traps	59
CLEAR-Flow	59
“show clear-flow vlan” Command Displays Invalid Threshold Type	59
CLEAR-Flow is Not Supported on Summit X450 and BlackDiamond 8800.....	59
CLEAR-Flow Does not Require a Space around Operators	59
CLEAR-Flow is Only Supported on BlackDiamond 10808 and BlackDiamond 12804 Systems	59
CLI	59
Load Script Unable to Process Banner Configuration	59
“show configuration” Command Output Includes Invalid Switch Prompt.....	59
Timezone/DST Name Truncates at Seven Characters.....	60
“show odometers” Command Does not Display PSUCTRL Service Days	60
RX Align Counter is not Incremented.....	60
“enable ipforwarding fast-direct-broadcast ignore-broadcast” Command is Not Supported ..	60
“upload configuration” Command Contains RIP Configuration Commands	60
“upload configuration” Command Generating Invalid CLI	60
“show ports mgmt utilization” CLI Command Does not Show any Statistics.....	60
Control Protocols.....	61
Switches Configured for VRRP can Experience State Changes.....	61
When a Port Link is Down or Disabled, UPM Should Register a Device-Undetect	61
Convergence Time May Increase After Removing Root Bridge from dot1s Network	61
Multiple BPDUs Sent From Root Port	61
CIST Ports Link-Type Configured as Point-to-Point Lost When Configuration is Uploaded and Downloaded.....	61
Summit X450a May Briefly Lose Data During a Failover	61
MSM Failover on ESRP Slave Running IGMP Causes Packet Loss	62
STP Blocks CFM Packets	62
Device Management	62
Specifying Port Numbers Does not Clear Number of Shared Ports from FDB Table.....	62
WAN-PHY Trace Path String Cannot be Longer than 16 Characters	62
DOS Console Window Does not Wait for User Input.....	62

ZX Mini-GBIC Appears as an LX Mini-GBIC on the Summit X450e-48p Switch.....	62
Extraneous Errors Displayed when Loading a Non-Existent Variable	62
Do not Use “configure-sys-recovery level slot” Command on MSMs	63
“show configuration” Command Output Shows Wrong Information	63
Diagnostics.....	63
Management Port Reported as Down in Shutdown State.....	63
sys-health-check Configurations are not Stored in Uploaded Configurations.....	63
EAPS	63
EAPS Loop Created when an EAPS Shared Port Partner Comes Up	63
Changing Shared Port Link ID When the Shared Link is Down.....	63
Traffic Loss Occurs When a Shared Link Comes Up	63
If Multiple Shared Links are Down, a Loop is Created	63
Number of EAPS Domains Supported by Advanced Edge License.....	64
Simultaneously Disabling Three Shared Port Links can Cause an EAPS Loop	64
EAPS Warning Messages are Displayed from VLAN Manager even after Turning Off	
Config-warnings	64
Disabling a Slot on a BlackDiamond 12804 Causes a Loop in EAPS Setup	64
EAPS with Load Sharing Enabled/Disabled Causes Control Packets to be Received on Port..	64
EAPS in Active Root Blocker State	64
ESRP	64
ESRP Slave Switch with Host Attach Ports does not have an ESRP Virtual MAC IP Address..	64
vMan Switches that act as ESRP-aware Cannot Forward Tagged ESRP Control Packets	65
MSM-Failover Causes ESRP Master Switch to Become ESRP Secondary Switch	65
MSM Failover from ESRP Master Causes an FDB Flush on new Master	65
VLAN Tracking Fails after an MSM Failover.....	65
Disabling a Shared Port Makes the ESRP Port Restart configuration disappears	65
Potential Problem with Graceful Disable of ESRP	65
Summit X450 Does Not Show all ESRP-aware Masters	65
IP Routing Protocols.....	65
Extreme Devices do not Support the PIM Prune Timer Option.....	65
“configure ipmroute” is not Applied Correctly on BlackDiamond 10808	66
IPv6 Multicast Flooding is Occurring in Software.....	66
ICMP Packets are not Answered Correctly	66
IGMP Memberships are Flushed if STP Link Goes Down.....	66
Packets Switched to SPT when TX Rate is Less than the SPT Threshold	66
MVR not Sending Periodic IGMP Reports.....	66
IGMPv3 Report Record Type "5" Message Does Not Work Correctly	66
unconfigure pim Command Removes SSM Configuration.....	66
IPv4 Capability Must be Configured for BGP Restart to Work Properly	66
show pim Command Should Return an Error Message When Protocol Not Added to User VR.	67
IPv4 Unicast.....	67
show platform ipv4Fib Command does not Support CLI Paging.....	67
IPv6 Unicast.....	67
Packets Forwarded Through Tunnels Do Not Use Fast Path	67
Neighbor Discovery Cache Allows Addition of Static Entry for Existing Address.....	67
IPv6 FIB and Adjacency Entries Cleared When Duplicate Address Detected	67
ICMPv6 Destination Unreachable Message Not Generated	67
Mirroring	67
Mirroring Port Should Not be Allowed in Load Sharing	67
Enabling Load Sharing on a Mirrored Port.....	68
MPLS.....	68
Router not able to Forward Multicast Traffic to its VPLS Peers.....	68
Router Address may Inadvertently be Purged from the OSPF Database	68
show mpls rsvp-te lsp detail Command may not Show Error Condition	68

Egress LSPs using Advertised Implicit NULL Labels are not Displayed	68
Changing Ethertype on VPLS Service vMAN Causes Traffic to Stop Forwarding.....	68
Configuring a VPLS Pseudo Wire ID of 0.....	69
MPLS does not Handle Restarting OSPF	69
Data Corruption and Subsequent Crash may Occur when Enabling and Disabling RSVP-TE...	69
Disabling and Enabling MPLS may Result in LDP Sessions Staying in a Non-Existent State..	69
SNMP Trap is not Generated for Blackholed FDB Entries	69
Dynamically Changing IP MTU can result in VPLS Sessions not Coming Up	69
Blackhole FDB Entries Incorrectly Adding when using VPLS MAC Limiting Feature.....	70
VPLS Limit Learning Causes FDB Entries Learned over VPLS to be Blackholed	70
Log Messages may be Generated during LSP Ping	70
Frames Exiting a Pseudo Wire are not Mirrored.....	70
When Disabling MPLS L2 VPN Log Messages may be Generated.....	70
Enabling or Disabling PHP on a VLAN does not Work if MPLS is Enabled	70
“show mpls ldp peer” Command does not Show Peer if Peer is Using an Interface Label Space	70
Disabling MPLS may Cause MPLS HAL Log Messages	70
Dynamically Configuring LDP to Advertise RIP Routes does not Work	71
VPLS Session Remains UP even if Configured to use a DOWN named LSP.....	71
Changing a VLAN from Tagged to Untagged may Result in LDP not Advertising a Label for that VLAN.....	71
nettx Logs When Trying to Forward 802.1Q Tagged Packets through VPLS.....	71
Globally Enabling IP Forwarding on all VLANs Incorrectly Results in IP Forwarding being Enabled on VPLS Service VLANs.....	71
Explicit NULL Labels are Treated as Implicit NULL Labels.....	72
VPLS and LSP Statistics—Do Not Include Counters from Ports Mapped to Backup MSM	72
The “clear counters” Command may Result in MPLS HAL Log Messages.....	72
Switch Experiences High Packet Loss.....	72
After Issuing run msm-failover Command Traffic Does not Completely Recover.....	72
Traffic Rate Drops over the VPLS Pseudo Wire after an MSM Failover.....	72
LDP Sessions Flap Because Hello Packets are not Periodically Sent after a Failover.....	72
LDP Path Vector Limit is not Working.....	72
LDP Path Vector Loop Detection may only Include Nexthop Path Vector LSR-ID.....	73
LDP Hop Count Loop Detection may not Work Properly	73
Packets with Router Alert Label (0x00001) are not being Forwarded.....	73
VLANs Configured as Protocol “any” Should be Added to MPLS	73
LDP Session does not Exit NonExistent State	73
ExtremeXOS does not Send back ICMP Responses for Traceroute through Non-Pipe Mode LSPs.....	73
LDP Should Not Advertise Certain Label Mappings	73
Labels for Static and RIP Routes not Advertised	73
MSM Failovers Displays Numerous Errors on Switch Console	74
EXP Field Examination and Replacement not Working	74
Sending LDP Labels and Stopping Transmission Causes Error	74
Pings and Traceroutes May not be Sent Using an LSP Even Though an LSP Next Hop is Available	74
LDP traffic needs to be prioritized.....	74
Multicast.....	75
Multicast Groups Continue to Age Out	75
No Entry for pimInterfaceTable When Configuring PIM.....	75
At Line Rates, a Large Percentage of IP Multicast Packets Sent to PIM RP Will be Dropped	75
show pim Command Only Counts Null-Registers.....	75
Multi-access VLANs with Two Upstream Neighbors Drop Assertion Messages	75

Network Login.....	75
"show netlogin" Command does not Display IP Address of 802.1X Supplicant	
Authenticated on Tagged Port.....	75
Network Login "move-fail-action" not Working Properly.....	76
Network Login Syslog Error Message	76
Network Login Client Needs to be Reauthenticated After flush-fdb.....	76
Guest VLAN Functionality does not Work Correctly with Multiple Supplicants.....	76
Web-based Network Login Authentication through Network Login Local User Database	76
Network Services.....	76
Ingress ACL "source-address 0.0.0.0/0" Matches Every Protocol Instead of IP Packets.....	76
Changing Traffic Queue Mode to Bandwidth Mode Requires Two Reboots	77
UPM Profiles Fail to Load	77
Disabling Sharing fills Console with Warning Messages	77
Configurations Using VR-Mgmt Interface as RADIUS Client IP Do Not Load	77
show ipstats ipv6 tunnel Command Shows All IPv6 Statistics	77
ARP Refresh Works Incorrectly When Default Value is Changed	77
IPv6 Configuration Changes Generate Error Messages	77
Enabled MLD Switches do not Reject Other Group Addresses	78
Hop-Limit in IPv6 Header is Ignored for Inbound MLD Packets.....	78
Telnet Requests Sent from MSM-A to MSM-B Causes MSM-A to Fail	78
Duplicate VLAN Tags will Cause Broadcast Packet to Drop	78
Creating Tagged vMANs and VLANs Using the Same Ports Sends Control Packets	
vMAN EtherType (0x88a8).....	78
Ingress Rate Limiting and Egress Rate Limiting are Mapping to Multiple Ports.....	78
vMAN ID ACL Translations May Fail with Transmit Errors	78
Checkpointing May Fail When Saving or Rebooting More than 4000 Traffic Queues.....	79
Converging MVR with EAPS on a BlackDiamond 8800 Causes a Large Packet Loss	79
Intra-vMAN Traffic Does not Forward on an Ingress ACL.....	79
Port-based Link Aggregation is not Currently Supported	79
Configuring a Meter Value not Working Properly on a BlackDiamond 12804.....	79
Load Sharing is not Working with MAC-in-MAC.....	79
Deleting an S-VLAN from a B-VLAN Generates an Error.....	79
Extreme Networks Uses the Value 0x88B6 for the Ethernet Type for CFM.....	80
Disabling Load Sharing May Cause Temporary State Change.....	80
Configuring an SSL Certificate Automatically Enables HTTPS	80
disable mld snooping Command Should not Have Dependency on IPv4 Forwarding	80
MLD Query Reverses Maximum Response Time and Last Member Query Interval	80
Switch May Stop Responding When Traffic Hits a Large ACL Policy	80
MLD Snooping Entry Not Created if VLAN Does Not Have an IPv6 Address	80
VLAN Statistic for rtif Interface is not Displayed	80
802.1P Precedence Support	80
Disabling Smart Redundancy.....	81
One Untagged port on Two VLANs with Different Protocols Can Cause Double Traffic.....	81
VLAN Mirroring Not Functioning Properly.....	81
Clearing Neighbor Cache Can Cause Packet Drops.....	81
Different Algorithm for IPMC Traffic Egress on a Trunk	81
OSPF	81
OSPF Process Not Starting After Running restart process ospf Command.....	81
OSPFv3.....	81
Changing Time While OSPFv3 is Learning Can Cause LSA to not Generate.....	81
Policy Manager	82
Incorrect Error Message When an Incorrect Policy is Configured Using BGP	82
Unsuccessful TFTP "Get" Removes the Existing File From the Switch	82

QoS	82
Bandwidth Mode HQoS Traffic Cannot be Limited	82
Changing the Default Queue Profiles	82
Disabling Load Sharing or Deleting Member Ports from a Trunk	82
RIPng	83
Cannot Bind Policy to RIPng Tunnel Interface.....	83
No Warning Message When Configuring More than 512 RIPng Interfaces	83
Malformed RIPng Packets	83
RMON.....	83
Restart and Terminate do not Support snmpMaster and snmpSubagent.....	83
Trap Community String Octet Limits for Agent is Not Correct.....	83
clear counter Command Not Supported	83
Alarm Entries Not Being Generated Correctly	83
Routing Protocols.....	84
PIM Cache not Created when VRRP IP Address is used as Gateway	84
Policies Configured on MVR Cannot be Refreshed	84
Security	84
Console Connection Allows Access to the Magic SysRq Facility.....	84
User ACL Given Higher Preference over EAPS System ACL	84
Portions of the IP Security Feature set are not Supported with Static IP Addresses	84
Load Script Defaults TACACS Configuration to VR-Mgmt.....	84
At Login, be Careful Entering Password after a Reboot	84
RSA Key not Supported	85
Enabling IP Security on Link Aggregation Ports is not Supported	85
Authentication Using Dummy Primary and Secondary Servers Fails.....	85
IP Security ACLs are not Shown for the show access-list vlan Command	85
DHCP Packets are not Relayed if dhcp-snooping violation-action is Set to None	85
RADIUS NAS-Port Attribute Should Display Without Slot Information.....	85
RADIUS NAS-Port Attribute is Missing for Network Login RADIUS Access Request Packets	85
unconfigure radius Command is not Clearing RADIUS Authentication and Accounting Counters.....	85
Unconfigure RADIUS and TACACS Does not Reset Timeout Value to System Default	86
RADIUS Authentication do not Work Correctly if Console Accesses the Backup MSM	86
icmpInMsgs Counter Displays only Incoming ICMP Packets.....	86
extremePortLoadshare MIB Table Empty When Load Sharing is Enabled.....	86
Changing a Password after Password Expiration Terminates SSH Session.....	86
ETHER-P-8021Q is Not a Valid Match Criteria	86
Upgrading and Rebooting a Backup MSM	86
sFlow	87
sFlow Will Accept Invalid IP Addresses for Collector Address	87
sFlow May Not Sample Correctly with Heavy Traffic	87
SNMP	87
SNMP MIB Query not Returning Consistent Value for Egress Port Bandwidth Use.....	87
Modifying IP Addresses through SNMP is not Possible.....	87
Smart Traps not Generated while Adding a Trap Rule IP Address	87
Some Objects in icmpGroup May Return Incorrect Values	87
alarmTable Does Not Validate the alarmVariable.....	87
Spanning Tree Protocol.....	88
CLI Does not Show a Clear Error Message when Configuring STP	88
When a Port Becomes an Alternate Port, the Switch does not send out an Alternate Proposal	88
CIST Ports Remain in Disabled State	88
Backup MSM Crashes When Disabling STP with MSTI and CIST Enabled	88
Removing MSTI Root or Making MSTI Root Inferior can Cause Topology Changes	88

Sending or Receiving Inferior BPDUs	88
SSH.....	88
ssh.xmod Must be Installed to Configure SSL Certificates	88
Uninstalling SSH Image Causes Watchdog Reboot.....	88
MSM-B Does Not Accept SSH Connection	89
Regenerating an SSH Key	89
Verify SSH Module and SSH Image are the Same	89
SSH2.....	89
DES Cipher Fails Authentication	89
System Related.....	89
Static Route Forwarding Does Not Forward to a Second Link	89
Disabling IP Forwarding on a VLAN	90
show log Error Messages	90
Unknown Card Type Error Message	90
UPM	90
LLDP is Showing Power in Tenths of a Watt	90
VLAN	90
SVLAN and BVLAN Cannot Share the Same Physical Port	90
VRRP	91
VRRP is not supported on User-Created VRs	91
MSM Failover on VRRP Backup Node Causes VRRP State Change	91
Configuring Advertised Intervals at 100 ms May Cause Dual Masters.....	91
Data Packets will not be Forwarded When Configuring VRRP with vrid >=7	91
High CPU Load Causes VRRP Flipping	91
XENPAK SR	91
When Changing Gigabit Links, the Link Light Being Up Does Not Guarantee Traffic Flow	91
Documentation	92
“configure vpls” Command Default for dot1q is Incorrect.....	92
“configure ospf import-policy” Command Does not Filter Routes.....	92
“show inline-power info detail” Command Output Differs from Documentation.....	92
“show inline-power” Command Output Differs from Documentation	92
Issues Resolved in ExtremeXOS 11.6.3.5.....	92
BlackDiamond 8800 Series of Switches	92
Issues Resolved in ExtremeXOS 11.6.3.4.....	92
BlackDiamond 8800 Series of Switches	93
Issues Resolved in ExtremeXOS 11.6.3.3.....	93
General	93
BlackDiamond 8800 Series of Switches	93
BlackDiamond 10808 Switch.....	94
BlackDiamond 12800 Series Switches.....	94
Summit Family of Switches.....	94
ACL	95
BGP.....	95
CLI	95
Control Protocols.....	95
Device Management	95
Documentation	96
EAPS	96
ESRP.....	96
IP Routing Protocols.....	97
IPv4 Multicast	97
MPLS.....	97
Network Tools	98

Network Services.....	98
OSPF	98
QoS	99
Security	99
sFlow	99
SNMP	99
Spanning Tree Protocol.....	99
SSH2.....	100
Stacking.....	100
vMAN.....	100
Issues Resolved in ExtremeXOS 11.6.2.9	100
General	100
BlackDiamond 8800 Series of Switches	100
BlackDiamond 10808 Switch.....	101
BlackDiamond 12800 Series Switches.....	101
Summit Family of Switches.....	101
ACL	101
CLI	102
Control Protocols.....	102
ELSM.....	102
ESRP	102
IP Routing Protocols.....	102
IPv6 Unicast.....	103
MPLS.....	103
Network Login.....	103
Network Services.....	103
Security	104
Spanning Tree Protocol.....	104
SSH2.....	104
Universal Port Management.....	104
vMAN.....	105
Issues Resolved in ExtremeXOS 11.6.1.9	105
General	105
BlackDiamond 8800 Series of Switches	105
BlackDiamond 10808 Switch.....	105
BlackDiamond 12800 Series Switches.....	105
Summit Family of Switches.....	106
ACL	106
CLI	106
Control Protocols.....	106
Device Management	107
DHCP.....	107
EAPS	107
ESRP	107
IP Routing Protocols.....	107
IPv6 Multicast	108
MPLS.....	108
Multicast.....	108
Network Login.....	108
Network Services.....	109

Network Tools	109
Security	109
Rapid Spanning Tree Protocol	109
Spanning Tree Protocol	109

1 Overview

These Release Notes document ExtremeXOS™ 11.6. ExtremeXOS 11.6 enables new hardware products and software features.

This chapter contains the following sections:

- [New Features in ExtremeXOS 11.6 on page 13](#)
- [Supported Hardware on page 17](#)

New Features in ExtremeXOS 11.6

Following are the new features supported in ExtremeXOS 11.6 or earlier. These features are documented in detail in the *ExtremeXOS Concepts Guide* or the *ExtremeXOS Command Reference Guide*, unless otherwise noted.

- SSH —public-key authentication



NOTE

This feature will be included in the ExtremeXOS Concepts Guide and the ExtremeXOS Command Reference Guide for ExtremeXOS 11.7.

Public-key authentication is an alternative method to password authentication that SSH uses to verify a client's identity. The client, or user, generates a key pair consisting of a private key and a public-key. The public-key is stored in the server, typically in the user's home directory. The server uses the public key to authenticate the user.

Limitations: Total number of keys—100; number of keys associated to a user—16.

Public-key authentication CLI commands

- **create sshd2 user-key <key_name> <key> {subject <subject>} {comment <comment>}**

<key_name> : Name of user's public key.

<key> : Key name in quotes.

<comment> : Comment in quotes. Optional.

<subject> : Subject in quotes. Optional.

This command is used to enter or cut and paste a user's public key.

- **delete sshd2 user-key <key_name>**

<key_name> : Name of user public key to delete.

This command is used to delete a user key. The key will be deleted regardless of whether it is bound to a user.

Example 1:

This command is used to associate/bind a user to a key.

```
delete sshd2 user-key id_dsa_2048
```

```
configure sshd2 user-key <key_name> add user <user_name>
```

<key_name> : Name of user's public key.

<user_name>: User associated to the key.

Example 2:

```
configure sshd2 user-key id_dsa_2048 add user admin
```

- **configure sshd2 user-key <key_name> add user <user_name>**

<key_name>: Name of user public key.

<user_name>: user to associate with the key.

Example:

```
configure sshd2 user-key id_dsa_2048 add user admin
```

This command is used to associate/bind a user to a key.

- **configure sshd2 user-key <key_name> delete user <user_name>**

<key_name> : Name of user's public key.

<user_name>: User to be unassociated with the key.

This command is used to unassociate or unbind a user from a key.

Example:

```
configure sshd2 user-key id_dsa_2048 delete user admin
```

- **show sshd2 user-key {<key_name> {users}}**

<key_name>: Name of user's public key. Optional.

user: Displays the name of the user bound to the key. Optional.

This command is used to indicate the number of user's bound to a key.

Example 1:

```
show sshd2 user-key
```

#*	Key_Name	Subject	Comment
2	Id_dsa_2048	joe	2048-bitdsa,joe@exos.extremenetworks.com, Tue Sep 26 2006
0	Id_rsa_2048	alex	2048-bitrsa,alex@exos.extremenetworks.com, Tue Sep 25 2006

* Indicates the number of user's bound to a key.

Example 2:

```
show sshd2 user-key Id_dsa_2048
```

```
---- BEGIN SSH2 PUBLIC KEY ----
```

Subject: joe

Comment: "2048-bitdsa,joe@exos.extremenetworks.com, Tue Sep 26 2006"

```
AAAAB3NzaC1kc3MAAAEBAMwqYfPpN4UsIhnDZ/AjnozjU/pU1fGFtAbTX/
Vblj4P3ow5oYyMdvzDC9dtjQ0EidyiZ4p6z78/
z2PE7zr38JDjEHLobUTazVhr392GieF2V6ezTcUZ5rwj
6P4m4yrMkwc2rn8ff9PbfNWi3KZ9EvWB/3wXlo+Ck//TGX2NXOX76Aj4qCwCfbVcd4Ubnz
2Y1yJfWK2K5PAMxXrMCXvk6tQVMGPEF4+q6HC9iQ9+KGHF5z0XVqWgVf0C4THMkbEQhoe7
DuVc1JN+jfFQnBZZJz/orLsQJpWJGDoCdfZ8knNI2lZjZtUbhU/
Sha8IYM6kXpsC929QjT3ozYWYVfymED0AAAAVAOjW/
bba+aEevcWwZ9wg3jqjVXG3AAABAQDAYNwQYUsCvGFIAag2dXSOeR2EuGliVol3ZB9U2yRM
zWJPPPvRvqlk5rpqtnxdHGaN9/MFyeO4lwd+Uz/
k5o9Rrl83DYRdOseqCVDEYC5iNsDntb2TIsVP0pluX6gEg37iUWxK04yul1mrjN999UUBFMQGqn
oZDWSqM1py2//OuaFZDBTFXep8gJVx821Q+K/
Y7ljQ2c7yFdv3Owk6RtPOkxrZiWXTc0peezo5WLUvED1BpAdQ+8QuOhZ608USyn92yXfrCU2+Y
O3IvmEwKYcV6LSnlPH6bCBE/q7CffEHSvTldBxCszMGvC6/
+JBvXhqsHTthL76D96MCwcfDz9YAAABAQCutdlRMxYXuE1xXFK1CYBgtitXJ5Py/
MRlwAqZ+SaxgeDbVLO+j1DPRI+WliCMXnLRK/5U+9kn21LyVdzutonOqYMTTUkkWJLQD/
```

```
aCWcgg1BTz9dAp4l98JRLaFswPpLLRzagjTVJqs1juCt08fPuMvDb08TH/
DiZw7AGyJ6HSpGzU2pwiU/
Oh5WA7u5xwKgQprytrxSyqrhuYrGwTzk7912kONG4ECC9dZsEyM9A4H9V0bk9h0z8Q8nSlv11
KTCXLWB5vwn4WNAw9/UA/
Gjzi+yd1Xie32owiyDi7FzzWxTqjMDQNsaXVVKyNzuHOSQl9fSVBwmkilDYJGBYGR7
---- END SSH2 PUBLIC KEY ----
```

Example 3:

```
show sshd2 user-key Id_dsa_2048 users
```

This example shows the number of users bound to key `Id_dsa_2048`.

```
admin
admin1
```

- **create sshd2 key-file [user-key <user_key_name> | host-key <host_key_name>]**

<user_key_name>: User public key to write.

<host_key_name>: Host public key to write.

This command writes a user or the host public key to the `/config/` directory. This is done so that the administrator can SCP the key files, after which the administrator can, and should, delete the file.

User key names are in the ExtremeXOS name space; the administrator can use CLI tab-completion to select a file.

The host/server key name is not in ExtremeXOS name space. An administrator will type in a name that will be used to write the key.

Example:

```
sshd write Id_dsa_2048
```

This writes the key to `Id_dsa_2048 .ssh in /config/`

- IPv6 forwarding in hardware for BlackDiamond® 8800 a-series and e-series I/O modules
- IPv4 Path MTU discovery and fragmentation for BlackDiamond 8800 a-series and e-series modules and Summit® X450a and X450e series switch
- Per-port jumbo frame support for BlackDiamond 8800 a-series and e-series modules and Summit X450a and X450e series switch
- Priorities for dynamic ACLs
- Access policy for SNMP
- 600/900 Watt AC PSU for BlackDiamond 8806
- 802.1D-2004 update
- Universal Port Manager (UPM)
 - Policies for static and dynamic port and device profiles
 - CLI scripting
- MPLS
 - LDP
 - RSVP-TE
 - CSPF
 - L2 VPLS
 - LSP Ping/Traceroute
- Bandwidth Resource Manager (BRM)
- Static multicast routes IPv4

- EAPS MIB enhancements
- IP Security
 - Disable ARP learning
 - DHCP snooping
 - Source IP lockdown
 - Trusted DHCP server
 - DHCP Option 82 VLAN ID
- MAC address security enhancement
 - Timeout option for lockdown
- Network Login
 - Dynamic VLAN creation on edge switches for edge and uplink ports
 - Port restart—port down for automatic client IP release for web-based Network Login
- VRRP enhancements
 - Hitless failover and process restart
- PR-CR mode for Hierarchical QoS (HQoS)
- Sentriant compatibility

Sentriant is an external security appliance used by the BlackDiamond 10808 and the BlackDiamond 12804 switches to detect and defend against threats without interfering with network traffic.

ExtremeXOS 11.6 is not tested with existing Sentriant revisions (2.3 and 2.4). You may lose your integration with Sentriant once you upgrade to ExtremeXOS 11.6.

Lab Supported Features in ExtremeXOS 11.6

QoS Monitor on BlackDiamond 8800 a-series and e-series Modules, and Summit X450a and X450e Series

The following command is introduced as a lab supported feature to display per QoS profile statistics:

```
show port <port> qosmonitor {no-refresh}
```

The following guidelines apply to the QoS monitor feature on these platforms:

- Only packet counters are available.
- You can monitor only one port per BlackDiamond 8800 module, or per Summit X450a series and Summit X450e series systems.
- If you attempt to monitor more than one port per BlackDiamond 8800 module, or per Summit X450a series and Summit X450e series system, the system returns the following error:

```
Error: Multiple ports on the same module cannot be monitored at the same time.
```

- If you issue the following command on an original BlackDiamond 8800 module, the system returns the following error message:

```
Error: Qosmonitor is not supported on MSM-G8X I/O ports and G48T, G48P, G24X, and 10G4X modules.
```

This command is not allowed on an original Summit X450 switch.

Supported Hardware

Refer to the *Extreme Networks Consolidated XOS Hardware Installation Guide* for more information about supported hardware. [Table 1](#), [Table 2](#), [Table 3](#), and [Table 4](#) list software filenames for the hardware that requires software.

BlackDiamond 10808 Component Support

BlackDiamond 10808 components supported with ExtremeXOS 11.6, and the minimum ExtremeXOS version required by the chassis to support each component, include:

Table 1: BlackDiamond 10808 Component Support

BlackDiamond Component	ExtremeXOS Filenames	ExtremeXOS Required	BootROM Version
MSM-1	bd10808-11.6.3.5.xos	10.1.0	1.0.1.5
MSM-1XL	bd10808-11.6.3.5.xos	10.1.0	1.0.1.5
10G2X	N/A	11.1.1	1.3.0.0
10G2H	N/A	11.2.0	1.3.0.0
10G6X	N/A	10.1.0	1.3.0.0
G20X	N/A	11.1.1	1.3.0.0
G60X	N/A	10.1.0	1.3.0.0
G60T	N/A	10.1.0	1.3.0.0
PSU Controller	N/A	1.0.1.0	N/A
700/1200 W AC PSU (Model # 60020/PS 2336)	N/A	10.1.0	N/A
1200 W DC PSU (Model # 60021/PS 2350)	N/A	1.0.1.0	N/A

BlackDiamond 8810 and BlackDiamond 8806 Component Support

BlackDiamond 8810 and BlackDiamond 8806 components supported with ExtremeXOS 11.6, and the minimum BootROM version required by the chassis to support each component, include:

Table 2: BlackDiamond 8810 and BlackDiamond 8806 Component Support

BlackDiamond 8810 Components	ExtremeXOS Filenames	ExtremeXOS Required	BootROM Version
MSM-G8X	bd8800-11.6.3.5.xos	11.1.1.9	1.0.1.7
G48Te	N/A	11.5.1.4	1.0.1.10
G48Pe	N/A	11.5.1.4	1.0.1.10
G48Ta	N/A	11.5.1.4	1.0.1.10
G48Xa	N/A	11.5.1.4	1.0.1.10
G48P	N/A	11.1.1.9	1.0.1.7
G48T	N/A	11.1.1.9	1.0.1.7
G24X	N/A	11.1.1.9	1.0.1.7
10G4X	N/A	11.1.1.9	1.0.1.7
10G4Xa	N/A	11.6.1.9	1.0.1.11

Table 2: BlackDiamond 8810 and BlackDiamond 8806 Component Support (Continued)

BlackDiamond 8810 Components	ExtremeXOS Filenames	ExtremeXOS Required	BootROM Version
PSU Controller	N/A	11.1.1.9	2.13
700/1200 W AC PSU (Model # 60020/PS 2336)	N/A	11.1.1.9	N/A
600/900 W AC PSU (Model # 41050/PS 2431) (BlackDiamond 8806 only)	N/A	11.6.1.9	N/A
1200 W DC PSU (Model # 60021/PS 2350)	N/A	11.3.2.6	N/A
MSM-48	bd8800-11.6.3.5.xos	11.6.1.9	1.0.1.11

**NOTE**

Upgrading the BootROM on a BlackDiamond 8810 or BlackDiamond 8806 switch is not automatic when you upgrade the software. You must be running the minimum required BootROM version or later. Use the install firmware command after upgrading the ExtremeXOS image to insure the BootROM is at the latest level.

BlackDiamond 12804 (R-Series) Component Support

BlackDiamond 12804 and BlackDiamond 12804 R-Series components supported with ExtremeXOS 11.6, and the minimum BootROM version required by the chassis to support each component, include:

Table 3: BlackDiamond 12804 Component Support

BlackDiamond 12804 Components	ExtremeXOS Filenames	ExtremeXOS Required	BootROM Version
MSM-5R	bd12k-11.6.3.5.xos	11.4.1.4	1.0.0.2
GM-20XTR	bd12k-11.6.3.5.xos	11.4.1.4	N/A
XM-2XR	bd12k-11.6.3.5.xos	11.4.1.4	N/A
MSM-5	bd12k-11.6.3.5.xos	11.4.1.4	1.0.0.2
GM-20XT	bd12k-11.6.3.5.xos	11.4.1.4	N/A
GM-20T	bd12k-11.6.3.5.xos	11.4.1.4	N/A
PSU Controller	N/A	11.1.1.9	2.13
700/1200 W AC PSU (Model # 60020/PS 2336)	N/A	11.4.1.4	N/A
1200 W DC PSU (Model # 60021/PS 2350)	N/A	11.4.1.4	N/A

Summit X450 Component Support

Summit X450 components supported with ExtremeXOS 11.6, and the minimum BootROM version required by the chassis to support each component, include:

Table 4: Summit X450 Component Support

Summit X450 Components	ExtremeXOS Filenames	Minimum ExtremeXOS Required	Minimum BootROM Version
Summit X450a Series			
Summit X450a-48t	summitX450-11.6.3.5.xos	11.5.1	1.0.2.2
Summit X450a-24t	summitX450-11.6.3.5.xos	11.5.1	1.0.2.2
Summit X450a-24tDC	summitX450-11.6.3.5.xos	11.5.1	1.0.2.2
Summit X450a-24xDC	summitX450-11.6.3.5.xos	11.6.1	1.0.2.2
Summit X450a-24x	summitX450-11.6.3.5.xos	11.6.1	1.0.2.2
Summit X450e Series			
Summit X450e-24p	summitX450-11.6.3.5.xos	11.5.1.4	1.0.2.2
Summit X450e-48p	summitX450-11.6.3.5.xos	11.6.1+	1.0.2.2
Summit X450 Series			
Summit X450-24x	summitX450-11.6.3.5.xos	11.2.2.4	1.0.0.9
Summit X450-24t	summitX450-11.6.3.5.xos	11.2.2.4	1.0.0.9
Option Cards			
XGM-2xn	summitX450-11.6.3.5.xos	N/A	N/A
XGM2-2xn	summitX450-11.6.3.5.xos	11.5.1	
XGM2-2xf	summitX450-11.6.3.5.xos	11.5.1	



NOTE

Upgrading the BootROM on a Summit X450 switch is not automatic when you upgrade the software. You must be running the minimum required BootROM version. Use the `download bootrom` command to download a BootROM image.

GBIC Support

GBICs supported on the BlackDiamond 10808 series switch with ExtremeXOS 11.6, and the minimum ExtremeXOS version required, include:

Table 5: BlackDiamond 10808 GBIC Support

GBIC	ExtremeXOS Required
SX parallel ID	10.1.0
SX serial ID	10.1.0
LX parallel ID	10.1.0
LX serial ID	10.1.0
ZX	10.1.0
ZX Rev 03	10.1.0

Table 5: BlackDiamond 10808 GBIC Support

GBIC	ExtremeXOS Required
LX70	10.1.0
LX100	10.1.0
UTP	10.1.0
SX SFP Mini	10.1.0
LX SFP Mini	10.1.0
ZX SFP Mini	10.1.0
1000BASE-T SFP Mini	11.1.1.9

GBICs supported on the BlackDiamond 8810 and BlackDiamond 8806 switch with ExtremeXOS 11.6, and the minimum ExtremeXOS version required, include:

Table 6: BlackDiamond 8810 and BlackDiamond 8806 GBIC Support

GBIC	ExtremeXOS Required
1000BASE-T SFP Mini GBIC	11.1.1.9
SX SFP Mini GBIC	11.1.1.9
LX SFP Mini GBIC	11.1.1.9
ZX SFP Mini GBIC	11.1.1.9
100FX/1000LX SFP Mini GBIC	11.3.1
100FX Mini GBIC	11.4.3.4 or 11.5.2.8 (not supported in 11.5.1.4)

GBICs supported on the Summit X450 switch with ExtremeXOS 11.6, and the minimum ExtremeXOS version required, include:

Table 7: Summit X450 GBIC Support

GBIC	ExtremeXOS Required
1000BASE-T SFP Mini GBIC	11.2.2.4
SX SFP Mini GBIC	11.2.2.4
LX SFP Mini GBIC	11.2.2.4
ZX SFP Mini GBIC	11.2.2.4
100FX/1000LX SFP Mini GBIC	11.3.1
100FX Mini GBIC	11.4.3.4 or 11.5.2.8 (not supported in 11.5.1.4)

XENPAK Module Support

XENPAK modules supported with ExtremeXOS 11.6, the minimum ExtremeXOS version required, and the manufacturers supported include:

Table 8: BlackDiamond 10808 XENPAK Support

XENPAK Module	ExtremeXOS Required	Manufacturers Supported
LR	11.1.1	Intel, Opnext
ER	11.1.1	Intel, Opnext

Table 8: BlackDiamond 10808 XENPAK Support

XENPAK Module	ExtremeXOS Required	Manufacturers Supported
SR	11.1.1	Intel
LX4	11.3.1	N/A
ZR	11.3.1	N/A
LRM-LR	11.4.1	N/A
LW ¹	11.4.1	Intel

¹ The LW XENPAK is supported only on the Summit X450a-24t and Summit X450a-48t switches.

XENPAK modules supported on the BlackDiamond 8810 and BlackDiamond 8806 with ExtremeXOS 11.6, the minimum ExtremeXOS version required, and the manufacturers supported include:

Table 9: BlackDiamond 8810 and BlackDiamond 8806 XENPAK Support

XENPAK Module	ExtremeXOS Required	Manufacturers Supported
LR	11.1.1	Intel, Opnext
ER	11.1.1	Intel, Opnext
SR	11.1.1	Intel
LX4	11.3.1	N/A
ZR	11.3.1	N/A
LRM-LR	11.4.1	N/A

XENPAK modules supported on the Summit X450 with ExtremeXOS 11.6, the minimum ExtremeXOS version required, and the manufacturers supported include:

Table 10: Summit X450 XENPAK Support

XENPAK Module	ExtremeXOS Required	Manufacturers Supported
SR	11.2.0	Intel
LR	11.2.0	Intel, Opnext
ER	11.2.0	Opnext
LX4	11.3.1	N/A
ZR	11.3.1	N/A
LRM-LR	11.4.1	N/A
LW ¹	11.5.1	Intel

¹ The LW XENPAK is supported only on the Summit X450a-24t and Summit X450a-48t switches.

XENPAKs not supplied by Extreme Networks will show up as “Unsupported Optic Module” in the `show port x:y` information detail and `show port x:y configuration` command output.

XFP Module Support

XFP modules supported on the Summit X450a and X450e series switch with ExtremeXOS 11.6, the minimum ExtremeXOS version required, and the manufacturers supported include:

Table 11: Summit X450a and X450e Series Switch XFP Support

XFP Module	ExtremeXOS Required	Manufacturers Supported
SR	11.5.1	Opnext
LR	11.5.1	Opnext

2 Upgrading to ExtremeXOS 11.6

This chapter contains the following sections:

- [Staying Current on page 23](#)
- [Upgrading ExtremeXOS on page 23](#)
- [Installing an ExtremeXOS Module on page 33](#)
- [Uninstalling an SSH Module on page 35](#)
- [Downgrading Switches on page 35](#)

Staying Current

If you are an Extreme Assist customer, the latest release and release notes are available after logging in to the Tech Support web site at

<http://www.extremenetworks.com/go/esupport.htm>.

For more information about ExtremeXOS, see the *ExtremeXOS Concepts Guide* and the *ExtremeXOS Command Reference Guide*.

Upgrading ExtremeXOS

Upgrading your current ExtremeXOS installation to ExtremeXOS version 11.6 is a multistep process. In this section is a quick summary of the necessary steps, followed by detailed instructions.



NOTE

See the “Hitless Upgrade Caveats for the BlackDiamond 8800 Series Switch Only” in the *ExtremeXOS Concepts Guide* for an important caution about performing an MSM failover.



NOTE

To upgrade to ExtremeXOS 11.6 you must currently be running ExtremeXOS 11.2.1 (or later). If you are not currently running that version, you must first follow the instructions in the ExtremeXOS 11.2.1 release notes to load that version of software.



NOTE

You can load ExtremeXOS software on the BlackDiamond 10808-series switch, the BlackDiamond 8800 family of switches, and the Summit X450 switch. BlackDiamond 8810 switches require version 11.1.1 or later, BlackDiamond 8806 switches require version 11.3.1 or later, BlackDiamond 12804 switches require version 11.4.1 or later, and the Summit X450 switches require a minimum of version 11.2.1. Summit X450a and Summit X450e series switches require ExtremeXOS 11.5 and higher.

Quick Summary

To install and upgrade to ExtremeXOS 11.6 on your system, you will be following these steps:

- 1 Download the image to your TFTP server.
- 2 Verify which virtual router connects to your TFTP server.
- 3 Save your configuration to a backup configuration file.
- 4 Determine your selected and booted image partitions.
- 5 Select the download partition and partition to use on reboot.
- 6 Download and install the image to the switch.
- 7 Reboot the switch.
- 8 Save the configuration for the new image.
- 9 Upgrade the BootROM—BlackDiamond 10808 switch only.
- 10 Upgrade the BootROM and PSU controller firmware—BlackDiamond 8800 family of switches only.
- 11 Upgrade the BootROM and PSU controller firmware—BlackDiamond 12804 family of switches only.



NOTE

If you have a dual MSM system, and the software image is not the same on both MSMs, see the section “Dual MSM Systems with Different Images Present” on page 32.

Detailed Steps



NOTE

Extreme Networks recommends using a TFTP server that supports blocksize negotiation (per RFC-2348). Using this type of server enables the switch to download the images faster.

To upgrade to ExtremeXOS 11.6 on your system, follow these steps:

- 1 Download the image to your TFTP server.
Download the image you received from Extreme Networks to your TFTP server.
- 2 Verify which virtual router connects to your TFTP server.
Use the following `ping` commands to test which virtual router you will need to specify when you download the image to your switch. This example assumes that your TFTP server's IP address is 192.168.0.12; substitute your own address when you issue the command:

```
ping vr vr-mgmt 192.168.0.12
ping vr vr-default 192.168.0.12
```


At least one of these commands must successfully reach your TFTP server for you to download the image. When you download the image in step 6, specify the virtual router that allowed you to reach your TFTP server.
- 3 Save your configuration to a backup configuration file.
You must save your configuration to a backup configuration file, or you will be unable to revert to your currently running image, if the need arises. In this example, we use the software version

number as part of the name. Use the following command to save the configuration to the file `version11_6_1_7.cfg`:

```
save configuration version11_6_1_7
```

As an optional, extra precaution, we suggest that you save this configuration to a TFTP server. Use the `tftp` command to save your configuration. In the following example, the TFTP server's IP address is `192.168.0.12`, the virtual router determined in step 2 is `vr-mgmt`, and the configuration file is `version11_6_1_7.cfg`:

```
tftp 192.168.0.12 -v vr-mgmt -p -l version11_6_1_7.cfg
```

4 Determine your selected and booted image partitions.

Issue the `show switch` command to determine your current selected and booted image partitions. The selected image partition indicates which image will be used at the next reboot. The booted image partition indicates which image was used at the last reboot.

Output from this command includes the version of the selected and booted images and if they are in the primary or the secondary partition. In this example, the selected and booted images are in the primary partition.

```
...
Image Selected:      primary
Image Booted:        primary
Primary ver:          11.6.1.7
Secondary ver:        11.6.1.7

Config Selected:     primary.cfg
Config Booted:        primary.cfg
```

5 Select the download partition and partition to use on reboot.

Specify the partition by issuing the following command:

```
use image pri
```

OR

```
use image sec
```

6 Download and install the image to the switch.

Download and install the image to the switch using the `download image` command. The virtual router `<vr>` that you will use is the one you determined in step 2. This example assumes that you are using virtual router `vr-mgmt` and TFTP server `192.168.0.12`, substitute your own virtual router and IP address when you issue the command:

```
download image 192.168.0.12 bd10808-11.6.3.5.xos vr vr-mgmt
```

(This may not be the actual filename; it is just an example.)

You will be asked:

```
Do you want to install image after downloading ? (y=yes, n=no, <cr>=cancel)
```

Answer `y`, for yes, so that the image will be installed after downloading.

7 Reboot the switch.

Use the `reboot` command to reboot the switch.



NOTE

For the BlackDiamond 8810 only—The first time the switch is rebooted after you upgrade to the 11.6 image, you will be prompted to upgrade the BootROM. Answer yes to the prompt.

8 Save the configuration for the new image.

Even though your configuration was saved before you rebooted, you will need to save the configuration with the new image. If you wait to login for some time after the reboot, you will receive a notice that recommends that you save the configuration. If you login soon after the reboot, you will not receive the notice, although an asterisk (*) will appear before the command prompt, indicating that the current configuration is not saved. In either case, save the configuration with the command:

```
save configuration
```

9 Upgrade the BootROM—BlackDiamond 10808 switch only.

Extreme Networks recommends that you upgrade to the latest BootROM for the BlackDiamond 10808. While not strictly required for this release, it is highly recommended. Run the `show version` command to verify the BootROM version currently running on your switch. If you are not running BootROM version 1.0.1.5 or later, upgrade the BootROM using the following command:

```
download bootrom 192.168.0.12 bd10808-1.0.1.5-bootrom.xbr
```

This example assumes that you will use the same TFTP server and virtual router as in step 6 above.

You will be asked if you want to install the BootROM after downloading. Answer yes, or use the `install bootrom` command to install later. Once the BootROM is downloaded and installed, it replaces the previous image stored in the onboard FLASH memory, and will be used at the next reboot.

10 Upgrade the BootROM and PSU controller firmware--BlackDiamond 8800 family of switches only.



NOTE

BootROMs installed by Manufacturing should never be forced to an earlier BootROM version unless explicitly instructed by Extreme Networks support.

Extreme Networks requires that you upgrade the MSMs, I/O modules, and PSU controllers in the BlackDiamond 8810 with the BootROM and firmware images included in this release of ExtremeXOS.

This release of ExtremeXOS contains the following versions of the BootROM and firmware:

MSM BootROM	1.0.1.11	First available in ExtremeXOS 11.6.1
I/O module BootROM	1.0.1.11	First available in ExtremeXOS 11.6.1
PSU controller firmware	2.13	First available in ExtremeXOS 11.4.1.4

Use the `show version` command to display the versions of the BootROM and firmware currently installed.

To install the new BootROM and firmware, wait until the `show slot` command indicates the MSMs and I/O modules are operational. Then use the `install firmware` command. This command will install the new BootROMs or firmware only on modules that have older BootROMs or firmware installed. You will be asked if you want to install each type of BootROM or firmware. New PSU controller firmware is used immediately after it is installed without rebooting the switch. The new BootROM and firmware overwrite the older versions stored in FLASH memory.

```
BD-8806.2 # install firmware
Installing version 1.0.1.11 of the MSM bootrom(s). Do you want to continue?
(y - yes, n - no, <cr> - cancel) Yes
Do you want to save configuration changes to primary.cfg? (y or n) Yes
Saving configuration on primary MSM ..... done!
Installing version 1.0.1.11 of the IO module bootrom(s). Do you want to continue?
(y - yes, n - no, <cr> - cancel) Yes
Installing version 2.13 of the PSU control module firmware. Do you want to
```

```

continue?
(y - yes, n - no, <cr> - cancel) Yes
Installing bootrom...
MSM bootrom(s) installed successfully
MSM bootrom(s) will be activated upon next MSM reboot
Installing bootrom...
IO module bootrom(s) installed successfully
IO module bootrom(s) will be activated upon next IO module reboot
Installing version 2.13 of the PSU control module firmware. Do you want to
continue?
(y - yes, n - no, <cr> - cancel) Yes
Installing firmware...
PSU controller firmware installed successfully
BD-8806.3 #

```

11 Upgrade the BootROM and PSU controller firmware--BlackDiamond 12804 family of switches only.



NOTE

BootROMs installed by Manufacturing should never be forced to an earlier BootROM version unless explicitly instructed by Extreme Networks support.

Extreme Networks requires that you upgrade the MSMs, I/O modules, and PSU controllers in the BlackDiamond 12804 with the BootROM and firmware images included in this release of ExtremeXOS.

This release of ExtremeXOS contains the following versions of the BootROM and firmware:

MSM Bootloader	1.0.0.3	First available in ExtremeXOS 11.4.1.3
PSU controller firmware	2.13	First available in ExtremeXOS 11.4.1.4

Use the `show version` command to display the versions of the BootROM and firmware currently installed.



NOTE

For single MSM systems, reboot the switch using the `reboot` command after the firmware installation is complete.

To install the new BootROM and firmware, wait until the `show slot` command indicates the MSMs and I/O modules are operational. Then use the `install firmware` command. This command will install the BootROMs and/or firmware only on modules that have older BootROMs or firmware installed. Once this installation is complete, reboot the switch using the `reboot` command.



NOTE

*For dual MSM systems, the `install firmware` command cannot install all the necessary software while the MSM is primary. To completely install the firmware, an MSM failover is required. First, run the `install firmware` command on the primary MSM. When the installation is complete, issue the `run msm-failover` command to allow the switch to failover to the secondary MSM. Run the `install firmware` command on the new primary MSM. To revert back to your original primary MSM, issue the `run msm-failover` command. Because two failovers are required for a dual-MSM firmware installation, you **will not** need to run the `reboot` command after executing the `install firmware` procedure.*

**NOTE**

Upgrading a BlackDiamond 12804 slot can take a minimum of six minutes per slot.

```
BD-12804.7 # install firmware
Installing version 1.0.0.2 of the MSM bootrom(s). Do you want to continue?
(y - yes, n - no, <cr> - cancel) Yes
Installing IO module firmware, a reboot is required. Do you want to continue?
(y - yes, n - no, <cr> - cancel) Yes
Installing version 2.13 of the PSU control module firmware. Do you want to
continue?
(y - yes, n - no, <cr> - cancel) Yes
Installing micro controller image on backup MSM requires rebooting backup MSM. Do
you want to continue?
(y - yes, n - no, <cr> - cancel) Yes
Installing bootrom...
Installing bootstrap
Installing active bootrom
Installing system FPGA image
Installing bootstrap
Installing active bootrom
Installing system FPGA image

MSM bootrom(s) installed successfully
MSM bootrom(s) will be activated upon next MSM reboot
Installing bootrom...
Installing microcontroller firmware to slot 1 ...
Installing FGPA firmware to slot 1. This will takes a few minutes...
Installing microcontroller firmware to slot 2 ...
Installing FGPA firmware to slot 2. This will takes a few minutes...
Installing microcontroller firmware to slot 5 ...
Installing FGPA firmware to slot 5. This will takes a few minutes...
Installing microcontroller firmware to slot 6 ...
Installing FGPA firmware to slot 6. This will takes a few minutes...
```

Upgrading ExtremeXOS on a Summit X450

Upgrade a Summit X450 switch to ExtremeXOS 11.6 as follows:

- 1 Save your configuration to a backup configuration file using the `save configuration` command.
You must save your configuration to a backup configuration file in order to revert to your currently running image if the need arises.
- 2 Download the latest image to the switch.
Download the image to the switch using the `download image` command. Download ExtremeXOS 11.6 image `summitX450-11.6.3.5.xos`.
- 3 Reboot the switch.
Use the `reboot` command to reboot the switch.

Upgrading the BlackDiamond Series of Switches Using Hitless Upgrade



NOTE

You must be running ExtremeXOS 11.1.1.9 or later to use hitless upgrade on a BlackDiamond 10808 switch.



NOTE

You must be running ExtremeXOS 11.4.1 or later to use hitless upgrade on the BlackDiamond 8800 series switch.



NOTE

For the BlackDiamond 8800 series of switches, attempting a hitless upgrade to ExtremeXOS 11.6.1 from an earlier release may fail during the download process. If this occurs, use the normal software upgrade.

Upgrading the Active Partition Using Hitless Upgrade

Upgrade the active partition using hitless upgrade as follows:

- 1 Issue the `show switch` command to determine which MSM is the primary and which MSM is the backup.
- 2 In the following example MSM-B is the backup.

```
Execute the CLI command download image 10.201.14.13 bd12k-11.6.3.5.xos msm b
* BD-12804.9 # download image 10.201.14.13 bd12k-11.6.3.5.xos msm b
Do you want to install image after downloading? (y - yes, n - no, <cr> - cancel)
Yes
Downloading to MSM-A.....
Downloading to MSM-B.....
Checking for possibility of hitless upgrade ...
done with success
Image will be installed to the active partition, a reboot required.
Do you want to continue? (y/n) Yes
```

When the download is complete MSM-B will reboot.

- 3 When MSM-B is up, issue the `show switch` command.
 - Verify that MSM-A is the master MSM, and MSM-B is the backup MSM and that BACKUP is followed by (In Sync).
 - Verify that “Image Selected” and “Image Booted” are both set for secondary on both MSM.
 - Verify that backup MSM-B displays new image version.

MSM:	MSM-A *	MSM-B
Current State:	MASTER	BACKUP (In Sync)
Image Selected:	secondary	secondary
Image Booted:	secondary	secondary
Primary ver:	11.4.1.4	11.4.1.4
Secondary ver:	11.4.1.4	11.6.2.9

4 Issue the `run msm-failover` command from MSM-A. MSM-B becomes the master MSM and MSM-A will reboot.

5 Run the `show switch` command.

- Verify that MSM-B is the master and MSM-A comes up as the backup. MSM-A will not become “in sync” with MSM-B.

Error messages related to conduits should be ignored.

- Verify that “Image Selected” and “Image Booted” are both set for secondary on both MSMs.

MSM:	MSM-A	MSM-B *
Current State:	BACKUP	MASTER
Image Selected:	secondary	secondary
Image Booted:	secondary	secondary
Primary ver:	11.4.1.4	11.4.1.4
Secondary ver:	11.4.1.4	11.6.2.9

6 Run the CLI command `download image 10.201.14.13 bd12k-11.6.3.5.xos msm a`

```
* BD-12804.9 # download image 10.201.14.13 bd12k-11.6.3.5.xos msm a
```

```
Do you want to install image after downloading? (y - yes, n - no, <cr> - cancel)
Yes
```

```
Downloading to MSM-A.....
```

```
Downloading to MSM-B.....
```

```
Checking for possibility of hitless upgrade ...
```

```
done with success
```

```
Image will be installed to the active partition, a reboot required. Do you want
to continue? (y/n) Yes
```

7 Once download completes MSM-A will reboot.

8 Once MSM-A comes up, run the `show switch` command.

- Verify that MSM-B is master and MSM-A comes up as the backup MSM, and displays (In Sync)
- Verify that “Image Selected” and “Image Booted” are both set for secondary on both MSMs.
- Verify that both MSMs display the new image version.

MSM:	MSM-A	MSM-B *
Current State:	BACKUP (In Sync)	MASTER
Image Selected:	secondary	secondary
Image Booted:	secondary	secondary
Primary ver:	11.4.1.4	11.4.1.4
Secondary ver:	11.6.2.9	11.6.2.9

9 Execute another `run msm-failover` so that MSM-A becomes the master. Run the `show switch` command to confirm.

MSM:	MSM-A *	MSM-B
Current State:	MASTER	BACKUP (In Sync)
Image Selected:	secondary	secondary
Image Booted:	secondary	secondary
Primary ver:	11.4.1.4	11.4.1.4
Secondary ver:	11.6.2.9	11.6.2.9

10 Run the `show version detail` command on MSM-A, which will display all of the I/O modules running the previous version (11.4.1.4) image, the MSMs however will be running the latest image. This version difference will cause no service disruption to the system as long as newer functionalities

from the latest image is NOT used. However it is highly recommended the I/O slot image is also consistent with the MSM version.

- 11 To upgrade the I/O module image to 11.6.3.5, run the `disable slot <slot number>` command followed by the `enable slot <slot number>` command. The `disable slot` command causes the I/O module to power down; the `enable slot` command causes the I/O module to power up.



CAUTION

Executing the `disable` and `enable` slot commands will cause service disruption until the slot is completely operational.

Upgrading the Alternate Partition Using Hitless Upgrade

Performing a hitless upgrade on the alternate partition allows you to revert to the previous image in case the upgrade is not successful. Upgrade the alternate partition using hitless upgrade as follows:

- 1 Issue the `show switch` command to determine which partition is the active partition and which partition is the alternate partition.
- 2 In the following example, the secondary image is the active partition. The download is performed on the primary image.

```
Execute the CLI command download image 10.201.14.13 bd12k-11.6.3.5.xos msm primary
* BD-12804.8 # download image 10.201.13.14 bd12k-11.6.3.5.xos primary
Do you want to install image after downloading? (y - yes, n - no, <cr> - cancel)
Yes
```

- 3 When the download is complete, run the `show switch` command to confirm the new image downloaded to the primary image.
- 4 Verify the following before rebooting the backup MSM:
 - “Primary ver:” is the image to be downloaded.
 - “Image Selected” is set to primary.

MSM:	MSM-A *	MSM-B

Current State:	MASTER	BACKUP (In Sync)
Image Selected:	primary	primary
Image Booted:	secondary	secondary
Primary ver:	11.6.2.9	11.6.2.9
Secondary ver:	11.4.1.4	11.4.1.4

- 5 Issue the `reboot` command to reboot MSM-B only.

```
reboot msm b
```

- 6 Run the `show switch` command to verify that:

- MSM-B is (In Sync) mode.
- “Image Selected” and “Image Booted” are both set for primary on the backup MSM.

MSM:	MSM-A *	MSM-B

Current State:	MASTER	BACKUP (In Sync)
Image Selected:	primary	primary
Image Booted:	secondary	primary
Primary ver:	11.6.2.9	11.6.2.9
Secondary ver:	11.4.1.4	11.4.1.4

- 7 Execute the `run msm-failover` command from the master MSM (MSM-A).
- 8 MSM-B becomes the master MSM, and MSM-A will reboot.
- 9 Run the `show switch` command to:
 - Verify that MSM-B is the master MSM and MSM-A is the backup MSM and displays (In Sync).
 - Verify that “Image Selected” and “Image Booted” are set for primary on both MSMs.

MSM:	MSM-A	MSM-B *
Current State:	BACKUP (In Sync)	MASTER
Image Selected:	primary	primary
Image Booted:	primary	primary

- 10 Run the `run msm-failover` command again so that MSM-A becomes the master MSM.

- 11 Run the `show switch` command to confirm the master MSM is now MSM-A.

MSM:	MSM-A *	MSM-B
Current State:	MASTER	BACKUP (In Sync)
Image Selected:	primary	primary
Image Booted:	primary	primary
Primary ver:	11.6.2.9	11.6.2.9
Secondary ver:	11.4.1.4	11.4.1.4

Dual MSM Systems with Different Images Present

If you have a dual MSM system that has different images on the MSMs, you will need to modify the upgrade procedure. One situation where you might have different images installed is when you add an MSM that has been in storage to your chassis, either for the first time, or as a replacement. You will only need to do the following procedure if one of the MSMs is running an image earlier than 11.0.0, and the images are different on the two MSMs (earlier versions of the software are unable to automatically synch up the configurations).

Follow the directions for upgrading the switch, and continue with step 6. When you download the image, as described in step 6, [Download and install the image to the switch.](#), you will be asked:

```
Do you want to install image after downloading ? (y=yes, n=no, <cr>=cancel)
```

Answer *n*, for no, so that the image will not be installed after downloading.

Next, manually install the image, using the following command:

```
install image bd10808-11.6.3.5.xos
```

Now the two MSMs have the same image installed, but may not have the same configurations. Reboot the secondary MSM using one of the following commands:

```
reboot msm b (if you are running on MSM A)
```

```
reboot msm a (if you are running on MSM B)
```

Finally, save the configuration on both MSMs by using the command

```
save configuration
```

Using a Rev 10 (or later) BlackDiamond 10808 MSM-1 or MSM-1XL



NOTE

To use a Rev 10 (or later) MSM-1 or MSM-1XL module, you must upgrade both the active and alternate images with the latest ExtremeWare 11.1.3 (or later) software image.

To determine which version of MSM you have installed in your switch, use the `show version` command.

If you have a Rev 9 (or earlier) MSM, the `show version` command output will look like this:

```
MSM-A :804015-00-09 0414F-00728 Rev 9.0 BootROM: 1.0.1.5 IMG:
```

If you have a Rev 10 (or later) MSM, the `show version` command output will look like this:

```
MSM-A :804407-00-10 0505F-00429 Rev 10.0 BootROM: 1.0.1.5 IMG:
```

Complete `show version` command output with Rev 10 MSMs will look like this:

```
BD-10808.2 #
BD-10808.2 # show version
Chassis      : 804300-00-03 0324X-00026 Rev 3.0
MSM-A        : 804407-00-10 0505F-00429 Rev 10.0 BootROM: 1.0.1.5 IMG:
MSM-B        : 804407-00-10 0505F-00431 Rev 10.0 BootROM: 1.0.1.5 IMG:
Image        : ExtremeXOS version 11.1.3.3 v11133 by release-manager on Thu Mar 31
19:12:57 PST 2005
BootROM      : 1.0.1.7
BD-10808.3 #
```

Installing an ExtremeXOS Module

An ExtremeXOS module has functionality that supplements a core image. You will download and install a module onto an already installed core image. The version number of the core image and the module must match. For example, the module *bd10808-11.6-ssh.xmod* can only be installed onto the core image *bd10808-11.6.xos*.

You can download and install the SSH module.



NOTE

You must terminate and restart the `thttpd` process before you can use SSL

Assuming that you have an installed and running ExtremeXOS 11.6 software on the active partition, follow these steps to install the module:

- 1 Download the module image to your TFTP server.

Download the image you received from Extreme Networks to your TFTP server.

2 Determine the active partition for your switch.

Issue the `show switch` command to determine your current selected and booted image partitions. The booted image partition indicates the currently active partition.

3 Download and install the module image to the active partition.

Download the image to the switch using the `download image` command. The filename for the only available module image is `bd10808-11.6.3.5-ssh.xmod`.

The virtual router `<vr>` that you will use is the one that connects to your TFTP server (you determined this in step 2, “Verify which virtual router connects to your TFTP server.” in the upgrade procedure). Since the system virtual router names changed from release 10.1.2.17 to 11.2.3.3, the name will be different from that used to download the initial upgrade image. Use `vr-mgmt` for this step or `vr-default`.

This example assumes that you are using virtual router `vr-mgmt` and TFTP server `192.168.0.12`, substitute your own virtual router and IP address when you issue the command:

```
download image 192.168.0.12 bd10808-11.6.3.5-ssh.xmod vr vr-mgmt <partition>
(primary or secondary)
```

You will be asked:

```
Do you want to install image after downloading? (y - yes, n - no, <cr> - cancel)
```

Answer y, for yes, so that the image will be installed after downloading.

4 Issue the `run update` command.

Issue the following command:

```
run update
```

The `run update` command starts up the processes associated with the new module, and makes them available to the system. You should now be able to issue the commands associated with SSH2.

You can verify that the SSH2 module is running by issuing the following command:

```
show process
```

If SSH2 is running, you will see a process named `exsshd` listed. You can then configure and enable SSH2 on the switch.

You can also verify that the SSH2 module is installed by issuing the following command:

```
show management
```

If the SSH module is installed, you will see text similar to the following:

```
SSH access : Disabled (Key invalid, tcp port 22 vr all)
```

If the SSH module is not installed, you will see text similar to the following:

```
SSH Access : ssh module not loaded.
```

Uninstalling an SSH Module

To uninstall the SSH module you must first terminate the THTTPD process:

- 1 Issue the `terminate process thttpd graceful` command. This terminates the THTTPD process.
- 2 Issue the `uninstall image bd10808-11.6-ssh.xmod <partition>` (primary or secondary) command. This uninstalls SSH from your switch.
- 3 Restart the `thttpd` process using the `start process thttpd` command.

Downgrading Switches

Following are the instructions for downgrading your ExtremeXOS version 11.6.1 installation to a previous version. It is assumed that you saved your configuration using the 11.4.1 image, and that the 11.4.1 image is currently installed on the switch, on the non-booted partition.



NOTE

Do not downgrade a BlackDiamond 8810 switch to an image earlier than 11.1.1 or a Summit X450 switch to an image earlier than 11.2.1. Do not downgrade a BlackDiamond 8806 switch to an image earlier than 11.3.1.1. Do not downgrade a Summit X450a or X450e switch to an ExtremeXOS image earlier than 11.5.1.

To downgrade to the existing ExtremeXOS version 11.4.1 image on your system, you will be following these steps:

- 1 Determine your selected and booted image partitions.

Issue the `show switch` command to determine your current selected and booted image partitions. The selected image partition indicates which image will be used at the next reboot. The booted image partition indicates which image was used at the last reboot.

Output from this command includes the version of the selected and booted images and if they are in the primary or the secondary partition. In this example, the selected and booted images are in the secondary partition.

```
...
Image Selected:      secondary
Image Booted:        secondary
Primary ver:         11.4.1.4
Secondary ver:        11.6.2.9

Config Selected:     primary.cfg
Config Booted:       primary.cfg
```

- 2 Select the reboot partition.

Assuming that the 11.4.1 image is on the non-booted partition, if you are currently running the image booted from the primary partition, issue this command:

```
use image secondary
```

If you are currently running the image booted from the secondary partition, issue this command:

```
use image primary
```

3 Select the reboot configuration.

Select the configuration to be used after reboot with the `use configuration` command. Assuming you saved the 11.4.1 configuration as *bdversion11_4_1_4.cfg*, use the following command:

```
use configuration bdversion11_4_1_4
```

4 Verify the image and configuration selection.

Again, issue the `show switch` command. The output should show that the selected image is the 11.4.1 image that you are downgrading to, and the selected configuration is the one you saved before you installed the 11.6.1 image:

```
...
Image Selected:   primary
Image Booted:     secondary
Primary ver:      11.4.1.4
Secondary ver:    11.6.2.9

Config Selected:  bdversion11_4_1_4.cfg
Config Booted:    primary.cfg
...
```

5 Reboot the switch.

Use the command `reboot` to reboot the switch.

3 Limits

This chapter summarizes the supported limits in ExtremeXOS.

Supported Limits

The table below summarizes tested metrics for a variety of features, as measured in a per-system basis unless otherwise noted. These limits may change but represent the current status. The contents of this table supersede any values mentioned in the *ExtremeXOS Concepts Guide*.



NOTE

See the *ExtremeXOS Concepts Guide* for information on which features are supported on each platform; see the specific section that discusses the specific feature.

Table 12: Supported Limits

Metric	Product	Limit
Access lists (policies) —suggested maximum number of lines in a single policy file.	BlackDiamond 10808	300,000
	BlackDiamond 12804	300,000
Access lists (policies) —maximum number of rules in a single policy file. ^a	BlackDiamond 8810	
	Original series modules (per GigE port)	128
	(per 10 GigE port)	1,016
	a-series modules	2,048
	e-series modules	1,024
	BlackDiamond 10808	30,000
	Summit X450	
	(per GigE port)	128
	(per 10 GigE port)	1,016
	Summit X450a-48t	
	per port groups 1-24 and 25-48	2,048
	Summit X450a-24t	2,048
	SummitX450e-24p	1,024
Access lists (masks) —maximum number of ACL masks per port. ^b	BlackDiamond 8800 series	16
	Summit X450	16

Metric	Product	Limit
Access lists (slices) —maximum number of field selectors for ACL slices.	BlackDiamond 8810	
	a-series modules per port groups 1-12, 25-36 and 13-24, 37-48	16
	e-series modules per port groups 1-12, 25-36 and 13-24, 37-48	8
	Summit X450a-48t per port groups 1-24 and 25-48	16
	Summit X450a-24t	16
	SummitX450e-24p	8
AAA (local) —maximum number of admin and local user accounts.	All platforms	16
BGP (aggregates) —maximum number of BGP aggregates.	All platforms	256
BGP (networks) —maximum number of BGP networks.	All platforms	1,024
BGP (peers) —maximum number of BGP peers.	BlackDiamond 8800 series	256*
	BlackDiamond 10808 (MSM-1XL)	512
	BlackDiamond 10808 (MSM-1)	256
	BlackDiamond 12804 (MSM-5R)	256*
	Summit X450	128*
	* With default keepalive and hold timers.	
BGP (peer groups) —maximum number of BGP peer groups.	All platforms	64
BGP (policy entries) —maximum number of BGP policy entries per route policy.	All platforms	256
BGP (policy statements) —maximum number of BGP policy statements per route policy.	All platforms	1,024
BGP (unique routes) —maximum number of unique BGP routes (LPM entries is limited to support TCAM entries on a BlackDiamond 10808).	BlackDiamond 8800 series	25,000
	BlackDiamond 10808 (MSM-1XL)	1,000,000
	BlackDiamond 10808 (MSM-1)	180,000
	BlackDiamond 12804 (MSM-5R)	225,000
	Summit X450	25,000
BGP (non-unique routes) —maximum number of non-unique BGP routes (LPM entries is limited to support TCAM entries on a BlackDiamond 10808).	BlackDiamond 8800 series series	25,000
	BlackDiamond 10808 (MSM-1XL)	2,000,000
	BlackDiamond 10808 (MSM-1)	900,000
	BlackDiamond 12804 (MSM-5R)	500,000
	Summit X450	25,000
BOOTP/DHCP relay —maximum number of BOOTP or DHCP servers per virtual router.	All platforms	4
Jumbo frames —maximum size supported for jumbo frames, including the CRC.	All platforms	9,216

Metric	Product	Limit
EAPS domains —maximum number of EAPS domains. Note: An EAPS ring that is being spatially reused cannot have more than four configured EAPS domains.	BlackDiamond 8800 series	32
	BlackDiamond 10808	128
	BlackDiamond 12804	128
	Summit X450	32
EAPSV1 protected VLANs —maximum number of protected VLANs.	BlackDiamond 8800 series	2,000
	BlackDiamond 10808	4,000
	BlackDiamond 12804	4,000
	Summit X450	1,000
EAPSV2 protected VLANs —maximum number of protected VLANs.	BlackDiamond 8800 series	1,000
	BlackDiamond 10808	4,000
	BlackDiamond 12804	4,000
	Summit X450	500
ELSM (ports per VLAN) —maximum number of VLANs per port.	BlackDiamond 8800 series	5,000
	BlackDiamond 10808	5,000
	BlackDiamond 12804	5,000
ESRP groups —maximum number of ESRP groups.	All platforms	7
ESRP domains —maximum number of ESRP domains.	BlackDiamond 8800 series	64
	BlackDiamond 10808	128
	BlackDiamond 12804	64
	Summit X450	64
ESRP VLANs —maximum number of ESRP VLANs.	BlackDiamond 8800 series	1,000
	BlackDiamond 10808	3,000
	BlackDiamond 12804	3,000
	Summit X450	1,000
ESRP (maximum ping tracks) —maximum number of IP route tracks per VLAN.	All platforms	8
ESRP (IP route tracks) —maximum IP route tracks per VLAN.	All platforms	8
ESRP (VLAN tracks) —maximum number of VLAN tracks per VLAN.	All platforms	1
Forwarding rate —maximum L2/L3 software forwarding rate.	BlackDiamond 8800 series (Mpps)	570
	BlackDiamond 12804	16,000
	Summit X450 (Mpps)	65
FDB (maximum L2/L3 entries) —maximum number of MAC addresses/IP host routes.	BlackDiamond 10808	224,000
	BlackDiamond 12804-R	224,000
	BlackDiamond 12804-non-R	49,000
FDB (maximum L2 entries) —maximum number of MAC addresses.	BlackDiamond 8800 series	
	(per I/O module)	16,384
	(per system)	128,000
	Summit X450 (per system)	16,384
	SummitX450a	16,384
	SummitX450e	8,192

Metric	Product	Limit
Hierarchical QoS —maximum number of ingress-only traffic queues per unit. (For 20XTR, first 10 ports ranges from 1 to 10 are UNIT-I, second 10 ports ranges from 11 to 20 are UNIT-II, for 10 Gig slot each port is one UNIT.)	BlackDiamond 12804-R	20,000
Hierarchical QoS —maximum number of ingress traffic queues with egress shaping allowed per switch.	BlackDiamond 12804-R	20,000
Hierarchical QoS —maximum number of egress-only traffic queues allowed per switch.	BlackDiamond 12804-R	30,000
Hierarchical QoS —maximum number of traffic queues attach per port.	BlackDiamond 12804-R	4,000
IGMP sender —maximum number of IGMP senders on an L2 configuration.	BlackDiamond 8800 series	500
	BlackDiamond 10808	15,000
	BlackDiamond 12804	15,000
	Summit X450	500
IGMP sender —maximum number of IGMP senders per switch.	BlackDiamond 8800 series	1,000
	BlackDiamond 10808	15,000
	BlackDiamond 12804	15,000
	Summit X450	1,000
IGMP v2 subscriber —maximum number of L2/L3 IGMP v2 subscribers per port.	BlackDiamond 8800 series	1,000
	BlackDiamond 10808	5,000
	BlackDiamond 12804	5,000
	Summit X450	1,000
IGMP v2 subscriber —maximum number of subscribers per switch.	BlackDiamond 8800 series	10,000
	BlackDiamond 10808	30,000
	BlackDiamond 12804	30,000
	Summit X450	10,000
IGMP v3 maximum source per group —maximum number of source addresses per group.	All platforms	250
IGMP v3 subscriber —maximum number of L2/L3 IGMP v3 subscribers per port.	BlackDiamond 8800 series	1,000
	BlackDiamond 10808	5,000
	BlackDiamond 12804	5,000
	Summit X450	1,000
IGMP v3 subscriber —maximum number of IGMP v3 subscribers per port.	BlackDiamond 8800 series	10,000
	BlackDiamond 10808	50,000
	BlackDiamond 12804	50,000
	Summit X450	10,000
IP ARP entries —maximum number of IP ARP entries.	All platforms	20,480
IP router interfaces —maximum number of VLANs performing IP routing - excludes sub VLANs	All platforms	512
IP static routes —maximum number of permanent IP routes.	All platforms	1,024

Metric	Product	Limit
IPv4 routes (LPM entries in hardware) — number of IPv4 routes in hardware. ^c	BlackDiamond 8800 series	25,000
	BlackDiamond 8810 a-series	12,000
	BlackDiamond 8810 e-series	460
	BlackDiamond 10808	256,000
	BlackDiamond 12804	229,000
	Summit X450	25,000
	Summit X450a	12,000
	Summit X450e	460
IPv6 routes (LPM entries in hardware) —number of IPv6 routes in hardware. ^b	BlackDiamond 8810 a-series	6,000
	BlackDiamond 8810 e-series	230
	BlackDiamond 10808	114,500
	BlackDiamond 12804	114,500
	Summit X450a	6,000
	Summit X450e	230
IP route sharing (maximum gateways) —maximum number of configurable gateways used by equal cost multipath static routes.	BlackDiamond 8800 series	4 or 8
	Summit X450	4 or 8
IP route sharing (total destinations) —maximum number of unique destinations used by multipath OSPF, OSPFv3, or static routes.	BlackDiamond 8800 series (default maximum gateways of 4) (if maximum gateways is 8)	511 255
	BlackDiamond 8810 a-series (default maximum gateways of 4) (if maximum gateways is 8)	511 255
	BlackDiamond 8810 e-series (default maximum gateways of 4) (if maximum gateways is 8)	32 16
	Summit X450 (default maximum gateways of 4) (if maximum gateways is 8)	511 255
	Summit X450 a-series (default maximum gateways of 4) (if maximum gateways is 8)	511 255
	Summit X450 e-series (default maximum gateways of 4) (if maximum gateways is 8)	32 16
	BlackDiamond 8800 series with 10G4X without 10G4X	32 128
	BlackDiamond 10808	128
	BlackDiamond 12804	128
	Summit X450	32
Load sharing groups —maximum number of load share groups.	BlackDiamond 8800 series	8
	BlackDiamond 10808	16
	BlackDiamond 12804	16
	Summit X450	8

Metric	Product	Limit
Logged messages —maximum number of messages logged locally on the system.	All platforms	20,000
MAC-based security —maximum number of MAC-based security policies.	All platforms	1,024
MAC-in-MAC —maximum number of MAC FDB entries (MAC addresses on the local side) and MAC binding entries (MAC addresses on remote side).	BlackDiamond 10808	100,000
	BlackDiamond 12804	100,000
MAC-in-MAC —maximum number of regular VLANs (VLAN, vMAN, BVLAN). No VLAN tag duplication support.	BlackDiamond 10808	4,000
	BlackDiamond 12804	4,000
MAC-in-MAC —maximum number of VLANs. (VLAN, vMAN, BVLAN, and SVLAN). VLAN tag duplication support on SVLANs.	BlackDiamond 10808 (1G DRAM)	16,000
	BlackDiamond 12804 (512 DRAM)	8,000
Mirroring (filters) —maximum number of mirroring filters.	All platforms	16
Mirroring (monitor port) —maximum number of monitor ports.	All platforms	1
MPLS configured interfaces —maximum number of MPLS configured interfaces per switch.	BlackDiamond 10808	16
	BlackDiamond 12804	10
MPLS LDP peers —maximum number of MPLS LDP peers per switch.	BlackDiamond 10808	16
	BlackDiamond 12804	12
MPLS LDP adjacencies —maximum number of MPLS LDP adjacencies per switch.	BlackDiamond 10808	50
	BlackDiamond 12804	50
MPLS LDP labels —maximum number of MPLS LDP labels per switch.	BlackDiamond 10808	20,000
	BlackDiamond 12804	5,000
IP multinetting (secondary IP addresses) —maximum number of secondary IP addresses per VLAN.	All platforms	64
Multicast VLAN registration (MVR) —maximum number of senders.	BlackDiamond 8800 series	500
	BlackDiamond 10808	15,000
	BlackDiamond 12804	15,000
	Summit X450	500
Network Login —maximum number of MAC-based Network Login clients per system.	BlackDiamond 8800 series (per module)	1,024
	Summit X450 (per system)	1,024
PIM—maximum mroutes —maximum number of IP multicast data streams.	BlackDiamond 8800 series	1,000
	BlackDiamond 10808	12,000
	BlackDiamond 12804	12,000
	Summit X450	1,000
PIM-SSM (maximum multicast groups) —PIM-SSM maximum mroutes/maximum number of IP multicast data streams.	BlackDiamond 8800 series	1,000
	BlackDiamond 10808	15,000
	BlackDiamond 12804	15,000
	Summit X450	1,000
OSPF adjacencies —maximum number of supported OSPF adjacencies.	BlackDiamond 8800 series	128
	BlackDiamond 10808	255
	BlackDiamond 12804	255
	Summit X450	128

Metric	Product	Limit
OSPF areas —as an ABR, how many OSPF areas are supported within the same switch.	All platforms	8
OSPF ECMP —maximum number of equal cost multipath OSPF.	BlackDiamond 8800 series (configurable) BlackDiamond 10808 BlackDiamond 12804 Summit X450 (configurable)	4 or 8 8 8 4 or 8
OSPF external routes —recommended maximum number of external routes contained in an OSPF LSDB without too many other types of OSPF routes.	BlackDiamond 8800 series BlackDiamond 10808 BlackDiamond 12804 Summit X450	20,000 130,000 130,000 5,000
OSPF inter- or intra-area routes —recommended maximum number of inter- or intra-area routes contained in an OSPF LSDB without too many other types of OSPF routes, with one ABR in OSPF domain.	BlackDiamond 8800 series BlackDiamond 10808 BlackDiamond 12804 Summit X450	7,000 7,000 7,000 2,000
OSPF routers in a single area —recommended maximum number of routers in a single OSPF area.	BlackDiamond 8800 series BlackDiamond 10808 BlackDiamond 12804 Summit X450	100 200 100 50
OSPF subnets on a single router —recommended maximum number of OSPF routed subnets on a switch.	All platforms	400
OSPF virtual links —maximum number of supported OSPF virtual links.	All platforms	32
OSPFv3 areas —as an ABR, the maximum number of supported OSPFv3 areas.	All platforms	16
OSPFv3 interfaces —maximum number of OSPFv3 interfaces.	BlackDiamond 8800 series BlackDiamond 10808 Summit X450	256 384 128
OSPFv3 neighbors —maximum number of OSPFv3 neighbors.	BlackDiamond 8800 series BlackDiamond 10808 BlackDiamond 12804 Summit X450	64 128 128 64
OSPFv3 virtual links —maximum number of OSPFv3 virtual links supported.	All platforms	16
OSPFv3 external routes —recommended maximum number of external routes.	BlackDiamond 8800 series BlackDiamond 10808 Summit X450	10,000 60,000 10,000
OSPFv3 inter- or intra-area routes —recommended maximum number of inter- or intra-area routes.	BlackDiamond 8800 series BlackDiamond 10808 Summit X450	6,000 6,000 3,000
Route policies —suggested maximum number of lines in a route policy file.	All platforms	10,000

Metric	Product	Limit
RIP-learned routes —maximum number of RIP routes supported without aggregation.	BlackDiamond 8800 series	10,000
	BlackDiamond 10808	10,000
	Summit X450	3,000
RIP interfaces on a single router —recommended maximum number of RIP routed interfaces on a switch.	BlackDiamond 8800 series	256
	BlackDiamond 10808	384
	Summit X450	128
Spanning Tree (maximum STPDs) —maximum number of Spanning Tree Domains on port mode EMISTP.	BlackDiamond 8800 series	64
	BlackDiamond 10808	64
	BlackDiamond 12804	64
	Summit X450	64
Spanning Tree PVST —maximum number of port mode PVST domains.	All platforms	128
Spanning Tree —maximum number of multiple spanning tree instances (MSTI) domains.	All platforms	64
Spanning Tree —maximum number of VLANs per MSTI.	All platforms	500
Spanning Tree —maximum number of VLANs on all MSTP instances.	All platforms	1,000
Spanning Tree (802.1d domains) —maximum number of 802.1d domains per port.	All platforms	1
Spanning Tree (number of ports) —maximum number of ports including all Spanning Tree domains.	All platforms	2,048
Spanning Tree (maximum VLANs) —maximum number of STP protected VLANs.	dot1d	560
	dot1w	560
SSH (number of sessions) —maximum number of simultaneous SSH sessions.	All platforms	8
Static MAC FDB entries —maximum number of permanent MAC entries configured into the FDB.	All platforms	1,024
Static multicast routes —maximum number of static multicast routes.	BlackDiamond 8800 series	256
	BlackDiamond 10808	256
	BlackDiamond 12804	256
	Summit X450	128
Syslog servers —maximum number of simultaneous syslog servers that are supported.	All platforms	4
TCAM entries —amount of entries available in the lookup tables for Longest Prefix Match routing lookups, learned MAC address, and ACLs.	BlackDiamond 10808, MSM-1	128,000
	BlackDiamond 10808, MSM-1XL	256,000
	BlackDiamond 12804 R-Series	229,000
	BlackDiamond non-R-Series	49,000
Telnet (number of sessions) —maximum number of simultaneous Telnet sessions.	BlackDiamond 10808	8
	Summit X450	8
Virtual routers —number of user virtual routers that can be created on a switch.	BlackDiamond 10808	8
	BlackDiamond 12804	8
	Summit X450	Not supported
VLANs —includes all VLANs.	All platforms	4,094
VLANs (Layer 2) —maximum number of Layer 2 VLANs.	All platforms	4,094

Metric	Product	Limit
VLANs (Layer 3) —maximum number of Layer 3 VLANs.	BlackDiamond 8800 series	512
	BlackDiamond 10808	512
	Summit X450	512
VLANs (maximum active port-based) —number of simultaneously active port-based VLANs.	All platforms	4,094
VLANs (maximum active protocol-sensitive filters) —number of simultaneously active protocol filters in the switch.	All platforms	15
vMAN (maximum ACL rules for vMAN) —maximum number of ACL rules for vMAN.	BlackDiamond 10808	4,000
	BlackDiamond 12804	4,000
VPLS VPNs —maximum number of VPLS virtual private networks per switch.	BlackDiamond 10808	500 point-to-point
	BlackDiamond 12804	500 point-to-point
VPLS peers —maximum number of VPLS peers per switch.	BlackDiamond 10808	16
	BlackDiamond 12804	16
VPLS pseudo wires —maximum number of VPLS pseudo wires per switch.	BlackDiamond 10808	1000
	BlackDiamond 12804	500
VPLS MAC addresses learned on VPLS pseudo wires —maximum number of MAC addresses learned on VPLS pseudo wires per switch.	BlackDiamond 10808	100,000
	BlackDiamond 12804	60,000
VRRP (maximum instances) —maximum number of VRRP supported VLANs for a single switch.	All platforms	128
VRRP (maximum VRID) —maximum number of unique VRID numbers per switch.	All platforms	7
VRRP (maximum VRIDs per VLAN) —maximum number of VRIDs per VLAN.	All platforms	7
VRRP (maximum ping tracks) —maximum number of ping tracks per VLAN.	All platforms	8
VRRP (maximum ping tracks) —maximum number of ping tracks per VRRP Instance under 128 VRRP instances. Hello interval: 100 milliseconds Frequency: 3 seconds Miss: 3	All platforms	2
	All platforms	4
VRRP (maximum ping tracks) —maximum number of ping tracks per VRRP Instance under 128 VRRP instances. Hello interval: 1 second Frequency: 3 seconds Miss: 3	All platforms	4
	All platforms	8
VRRP (maximum iproute tracks) —maximum number of iproute tracks per VLAN.	All platforms	8
VRRP —maximum number of VLAN tracks per VLAN.	All platforms	8

- a. The table shows the total available, but see the note “Summit X450a and Summit X450e series switches and BlackDiamond 8800 a-series and e-series Modules: Boot Time and Timing for Applying ACLs” on page 56.

- b. An ACL mask defines a unique match criteria and relative rule precedence. Masks are automatically generated based on the contents of an access-list policy. Only adjacent rules within the policy that have identical match criteria will utilize the same ACL mask. For this reason, it is advantageous to list all rules with the same match criteria together unless a relative precedence with other policy rules is required. Using VLAN-based or wildcard ACLs requires the ACL masks to be allocated on every port in the system.
- c. On a BlackDiamond 8800 series or Summit X450, it is not advised to have greater than 25,000 total IP routes. Adverse effects can occur with routing tables larger than this, especially when a single network event or CLI command affects a significant number of routes. For example, just after such a network event, the added system load will cause a “save configuration” command to time out.

This chapter describes items needing further clarification and behaviors that might not be intuitive. Numbers in parentheses are for internal reference and can be ignored.

This chapter contains the following section:

- [Clarifications and Known Behaviors on page 47](#)
- [Issues Resolved in ExtremeXOS 11.6.3.5 on page 92](#)
- [Issues Resolved in ExtremeXOS 11.6.3.4 on page 92](#)
- [Issues Resolved in ExtremeXOS 11.6.3.3 on page 93](#)
- [Issues Resolved in ExtremeXOS 11.6.2.9 on page 100](#)
- [Issues Resolved in ExtremeXOS 11.6.1.9 on page 105](#)

Clarifications and Known Behaviors

Following are the clarifications and known behaviors for supported features in ExtremeXOS 11.6. They are organized into the following sections:

General

UPM Profiles may take a Long Time to Execute

To recover from loops in scripting, or commands that take an excessive amount of time to execute, any profile that is run for more than 30 seconds will be terminated. The message "Possible loop condition" is logged in EMS (PD3-109903252).

Do not use the “configure sys-recovery-level none” Command

The `configure sys-recovery-level none` command can cause the system to behave incorrectly after a process failure. Use this command in this mode only if working directly with Extreme technical support (PD3-77427318).

Do Not Configure Conflicting System Recovery Levels

System recovery does not occur when configuring `sys-recovery-level none` in the software and `shutdown` in the hardware on Summit X450a and Summit X450e switches. For example, if you configure the following conflicting commands:

```
configure sys-recovery-level none
configure sys-recovery-level switch shutdown
```

The switch does not shutdown when a hardware error occurs (PD3-77236982).

10 Gigabit Port Shows Local Fault and Link Down in Syslog When Rebooting

When booting up an I/O module, the switch consistently logs a local fault and link down error in the syslog for 10 gigabit ports (PD3-40858541).

Process is Lost if Configuration Saved After Terminating Process

After terminating a Network Login process (or any other process), the `show configuration` command shows the current configuration; however, after issuing the `save configuration` command, the configuration is lost (PD3-40795350).

Saving an SSL Configuration

Saving an SSL configuration causes temporary high CPU utilization (PD3-29034131).

BlackDiamond 8800 Series of Switches

Disable RIP Commands Sometimes Causes CLI to Hang

On a BlackDiamond 8800 series switch with a G48T module, the `disable rip` command sometimes causes the CLI to hang (PD3-128654641).

“configure vlan protocol ipv6” Command Does not Display

The `configure vlan protocol ipv6` command does not display in the `show configuration` command output even though it is displayed in the `show vlan` command output (PD3-125375611).

Hot Swapping an I/O Module Allows Link Peer to Get an Active Link State

Hot swapping a 10G4X or G24X I/O module in a BlackDiamond 8810 allows the link peer to prematurely get an active link state. If this port is configured as an EAPS shared port, a temporary loop is also seen in the network. This problem has been corrected on G48Xa and 10G4Xa modules only (PD3-60122761).

RX Over Counter is not Incremented on a BlackDiamond 8800 Switch

For ports on Summit X450 switches and BlackDiamond 8800 MSM-G8X, G48T, G48P and G24X modules, the RX Over counter is not incremented when ports are connected at 100Mbps. The RX CRC counter is incremented instead (PD3-86869211).

Conduit Receive Error May Occur on MSM Failover

A conduit receive error may occur on MSM slots when performing an MSM failover (PD3-94962493).

OSPFv3 Can Lose Adjacencies with IPv6 traffic

IPv6 traffic is slow path forwarded while ingressing on the BlackDiamond 8800 original series modules. Conditions can arise in which the CPU is unable to keep up with both the IPv6 traffic and the OSPFv3 handshaking, and in turn, adjacencies may be lost (PD3-78998371).

Removing the Primary MSM to Initiate Failover Causes Module is Removed Messages to Appear in the Log

If you have a mix of BlackDiamond 8800 original, a-series, and e-series modules installed and remove the primary MSM to initiate failover, informational messages similar to the following appear twice in the log:

```
<Info:HAL.Card.Info> MSM-B: Module in slot 5 is removed
```

Since you removed the primary MSM only once, you should see this message once, not twice (PD3-77979043).

Hitless Upgrade not Supported

If you are running ExtremeXOS 11.4 or earlier, do not attempt to perform a hitless upgrade to ExtremeXOS 11.5 or later. On the BlackDiamond 8800 series switch, these versions of software are incompatible and cannot exist on MSMs installed in the same chassis even during the hitless upgrade process (PD3-78960359).

When Routing, Ingress Mirrored Traffic is Modified for Routing

When routing between VLANs on a BlackDiamond 8800 original series or Summit X450 series switch, ingress mirrored traffic is presented to the monitor port as having been modified for routing (PD3-45929245).

Delay in Displaying FDB Entries

It can take up to 10 seconds to re-learn an FDB entry after clearing the FDB on a BlackDiamond 8800 series switch (PD3-30082108, PD3-24090253, PD3-17993130).

Untagged VLAN Should Drop Packets

On a BlackDiamond 8810 switch, configure one ESRP domain on VLAN1 and VLAN2 respectively. Disable ESRP on VLAN1, and enable ESRP on VLAN2. On VLAN1, send IP packets with the destination MAC being ESRP virtual MAC. Some packets are forwarded by the CPU (PD3-42689279, PD3-29694962).

BlackDiamond 10808 Switch

BlackDiamond Using 64 ESRP Domains/512 VLANs Generates HAL Core

A BlackDiamond 10808 using 64 ESRP domains and 512 VLANs, the HAL core is generated during the `save` and `reboot` commands (PD3-93088150).

System Health Check Parity Walk Verification Function Should be Enabled

Various memory locations that are part of the forwarding and routing tables are parity protected on BlackDiamond 10808 switches. The functionality should be turned on so that faults are detectable (PD3-68165111).

Output for the "show platform ipv4mc group <group address>" Command Contains an "invalid" Entry

The command output for the `show platform ipv4Mc group <group address>` command contains an "invalid" entry.

```
BD-10808.61 # show platform ipv4Mc g 239.255.255.1
Total Entries:27
Index      Type VrId  Port   Source Group PTI Vlan
004A6 -> 03E3A [3] - invalid
(PD3-41204902, PD3-30483791)
```

BlackDiamond 10808 Crashes with G60T Module

If you enable SSH, create a virtual router, enable SSH on the virtual router, and then remove the virtual router on a BlackDiamond 10808 switch with a G60T module, the switch may crash.

Workaround. Remove all services associated with the virtual router, such as OSPF, BGP, PIM, RIP, and so on, before removing the virtual router.

(PD3-63362121)

I/O Modules Fail Due to a Conduit Ping Timeout

I/O modules on a BlackDiamond 10808 with a total of 24,000 OSPF and BGP routes with data traffic may fail due to conduit ping timeout after an MSM failover (PD3-59273325).

Incorrect Warning in the Log About the MSM Type

The following warning message is found in the log when configuring an MSM using the incorrect MSM type:

```
09/17/2005 15:41:34.94 <Warn:DM.Warning> MSM-B: MSM-A is of type MSM-1XL which is
not checkpoint compatible with MSM-B
(PD3-47375039)
```

BlackDiamond 10808 May Reboot When All PSUs Experience a Brownout

When all active PSUs on a BlackDiamond 10808 experience a brownout from 220 V AC to 110 V AC at the same time, the switch may reboot (PD3-46512388).

Dual Speed 100FX/1000LX SFP Lights When Inserted Without a Link

Dual speed 100FX/1000LX SFP is not supported on a BlackDiamond 10808 switch, however, dual speed 100FX/1000LX SFP should not light when inserted without a link (PD3-39759471).

Intel LR XENPAK Module is not Displaying Correctly

The Intel LR XENPAK module is displaying as an SR module on the BlackDiamond 10808 switch (PD3-41080591).

Opnext ZR XENPAK Module is not Displaying Correctly

The Opnext ZR XENPAK module is displaying as an SR module on the BlackDiamond 10808 switch (PD3-36734601).

Intel ER and Intel LR XENPAK Modules are not Displaying Correctly

The Intel ER and Intel LR XENPAK modules are displaying as SR modules or unsupported on the BlackDiamond 10808 switch (PD3-37075321).

Shared Portion of the (TCAM) Memory Blocks Cannot be Reclaimed

Once the shared portion is allocated to one resource type, such as an FDB or ACL, it cannot be reclaimed to be used for other resource type entries (PD3-7347167, PD2-199490211).

Hot Swapping the Master MSM

Hot swapping the master MSM may generate the following message:

```
WKNINFO: Invalid self slot number 0
```

(PD3-17230511)

Overflowed Routes and Entries are not Installed Automatically

When TCAM space becomes available after an overflow situation, the overflowed routes and entries are not installed automatically (PD2-238395030).

BlackDiamond 12800 Series Switches

MSM B is taking too Long to Come Up

After rebooting a BlackDiamond 12804 with continuous traffic flowing, MSM B is taking too much time to come up (PD3-126533672).

Disabling and Enabling a Port Can Take 30 Seconds for Port to Activate

During continuous FDB learning, disabling/enabling a port can take up to 30 seconds for the port to activate (PD3-98333969).

I/O Modules take too Much Time to Become Operational

Running the `clear slot` command on a system with large configurations takes a long time to process. Based on the configuration, it may take more than one minute for the cleared slot to become operational (PD3-67969258, PD3-61635051).

ESRP Master Change from BlackDiamond 12804 to BlackDiamond 8800

Changing the ESRP master from a BlackDiamond 12804 to a BlackDiamond 8800 or Summit X450 causes a traffic loss of more than eight seconds (PD3-62724747, PD3-56223462).

Packet Loss Occurs When A BlackDiamond 12804 Becomes ESRP Master

When ESRP is running on a BlackDiamond 12804 and a BlackDiamond 8800, there is a three second traffic loss when the BlackDiamond 12804 becomes the master rather than the BlackDiamond 8800 (PD3-56812371).

Downloading an Image Generates Errors in Log

Downloading an a new image on a BlackDiamond 12804 generates the following log message multiple times:

```
<Crit> MSM-A.ems:  !!!!!!!!!!!!!!!!!!!!!!!!!!!!! Kernel thread is stuck for 1.78 seconds
jiffies: 484732
<Info> MSM-A.nodemgr: perfTimer select (x33516 0%):  Flags=0002 Min :  0.000000
0.000000  0.000000 0 0 0 0 0 0 0 0 0 0 0 0 0 0 Avg :  0.134964  0.000000
0.000000 0 0 0 0 0 0 0 0 0 0 0 0 0 0 Max :  1.770000  0.000000  0.010000 0 0 0 0
0 0 0 0 0 0 0 0 0 0
```

(PD3-63913145)

BlackDiamond 12804R Enables All Ports at Initial Bootup

At initial bootup, the BlackDiamond 12804R prompts a user as to whether or not to disable all ports on the switch. After the initial bootup, all ports are enabled until the user responds to `disable all ports`. All ports should be disabled after initial bootup until the user responds to `enable all ports` (PD3-63887081).

Backplane Link to Backup MSM Message is not Correct

Since the backup MSM does not have access to I/O modules until the backup MSM becomes the master, the following message should be deleted:

B - Backplane link to Backup MSM is also Active


```
* BD-12804.1 # show slot
Slots      Type      Configured  State      Ports      Flags
-----
Slot-1     XM-2XR     XM-2XR     Operational 2          MB
Slot-2     XM-2XR     XM-2XR     Operational 2          MB
Slot-5     GM-20XTR  GM-20XTR  Operational 20         MB
Slot-6     XM-2XR     XM-2XR     Operational 2          MB
MSM-A      MSM-5R
MSM-B      MSM-5R
Operational 0
Operational 0

Flags:  M - Backplane link to Master MSM is Active
        B - Backplane link to Backup MSM is also Active
        D - Slot Disabled, S - Slot Secured
        I - Insufficient Power (refer to "show power budget")
* BD-12804.2 #
```

(PD3-62516612)

“show version” Command May Display Old Firmware Versions

The `show version` command may display the old firmware version if you run the command between the `install firmware` command and the `reboot` command on a BlackDiamond 12804 (PD3-62187218).

Summit Family of Switches

Summit Switch Logs a Link Down Event with Local Fault

A Summit X450 series switch logs a link down event showing Local fault as the reason for the event. The link down event applies to each 10G XENPAK port present on reboot when the cable is connected to both the local (near-end) and remote (far-end) ports.

```
X450e-24p.1 # show log
02/20/2007 19:32:16.89 <Info:vlan.dbg.info> Port 26 link up at 10 Gbps speed and
full-duplex
02/20/2007 19:32:16.79 <Info:vlan.dbg.info> Port 25 link up at 10 Gbps speed and
full-duplex
02/20/2007 19:32:16.36 <Info:vlan.dbg.info> Port 26 link down due to local fault
02/20/2007 19:32:16.35 <Info:vlan.dbg.info> Port 25 link down due to local fault
```

This message can be ignored (PD3-127957781).

Shared Port Link Comes up Before the Software is Initialized

After a Summit X450a-24x switch reboots, the shared port link comes up before the software is initialized, resulting in traffic loss (PD3-140632406).

On Rebooting SummitX450-24x, Neighboring Switches may see a Link Flap

When rebooting a SummitX450-24x, neighboring switches connected to the fiber port may see a link flap before the switch is in the operational state. This could result in a transient change to the state of protocols such as EAPS (PD3-89711032).

Disabling and Enabling a 100FX Module Displays Wrong Speed

On a Summit X450 switch, when autonegotiation is On, disabling and enabling a port on a 100FX module displays the wrong speed. This is only supported when autonegotiation is set to Off (PD3-103618060, PD3-95143042).

Port Number Display is Misleading in Messages

Some error and warning messages display a misleading port number. For example, if you configure a duplicate receiver port on the MVR VLAN mc4, using the following command:

```
configure mvr mc4 add receiver port 1
You will see the following error message:
MVR receiver port 256:2 already configured on Vlan mc4
```

(PD3-78947315)

L3 Algorithm Flags can be Ignored in the “show ports sharing” Command Output

On the Summit X450a and X450e series switches, you can ignore the "L3" algorithm flags displayed in the `show ports sharing` command output. These switches currently support the Layer-2 and Layer-3_Layer-4 combination algorithms (PD3-77978516).

Clearing the System Recovery Level Generates Erroneous Log Messages

If you use the `clear sys-recovery-level` command on the Summit X450a and X450e series switches, a message similar to the following appears in the log:

```
<Warn:DM.Warning> devmgr does not have a connection to Backup to checkpoint
```

You can safely ignore this message; it does not affect system operation (PD3-78030636).

Management Port Reported as Down in the Shutdown State

The management port is reported as down in when it is in the shutdown state but it is actually working correctly. When the Summit X450 switch is in shutdown state, all ports must be down with the exception of the management port (PD3-87341149, PD3-77237152).

Reconfiguring the vMAN Ethernet Type is not Effective Until Shared Port is Deleted and Added

Reconfiguring the vMAN ethertype value from 0x8100 to a value other than 0x8100 will not become effective until disconnecting and adding back the port being shared by the vMAN and VLAN. This means the EtherType value remains 0x8100 even though the `show vMAN eth` command shows the re-configured value (PD3-75224031).

Load-Sharing Port Removed from STP Domain Without Warning

When load sharing is disabled, the STP related configurations on the load shared ports will be lost (PD3-76234725).

“Slot” Should not be Included in “show inline-power stats” Command Output

The word “slot” should not be included in the output of the `show inline-power stats` command (PD3-77711011).

Priority Column Should not be Included in “show inline-power configuration” Command Output

The Priority column should not display in the output of the `show inline-power configuration` CLI command when running the command on a Summit 24p PoE switch (PD3-77711042).

“save configuration” Command Must be Performed After Setting Sys-Health-Recovery Level to Shutdown

It is necessary to save your configuration after configuring sys-health-recovery level to shutdown to ensure proper operation of the feature. Recovery from a hardware failure will cause a Summit switch to reboot. You must save the configuration to ensure the proper system behavior (PD3-98415064).

“show log” Command Output Filled with sFlow Receiver Missing Message

If sFlow does not have a collector configured using the `configure sflow collector` command, the `show log` command generates the following messages:

```
08/23/2005 12:28:09.55 <Noti:sflow.debug.AddCntSmplFail> : Could not add the counter
sample for port 0:1020, as receiver is not configured.
```

```
08/23/2005 12:07:49.55 <Noti:sflow.debug.AddCntSmplFail> : Previous message repeated
61 additional times in the last 1200 second(s).
```

(PD3-43606168)

Dot1p-Based QoS Mapping Priority Error

Dot1p-based QoS mapping is taking a higher priority than ACL-based mapping.

Workaround. Allow more than one ACL rule in non-conflicting conditions.

(PD3-34629895, PD3-22630366)

Redundant Ports not Correctly Moving to Other Ports in Load Sharing Mode

Traffic on load share ports configured as redundant ports incorrectly moves to other ports in the load share group during link transition (PD3-40266236, PD3-40233121).

“restart ports” Command Runs Too Quickly on a Summit X450

Connecting a Summit X450 to a BlackDiamond switch and issuing the `restart ports` command from the Summit X450, the Summit X450 log shows that the link was brought DOWN and UP in 0.5sec, but the BlackDiamond switch does not see the link UP/DOWN state (PD3-34629664, PD3-25415431).

Flow Control is Always Reported for 1000 Mbps Link Speed

When a Summit X450 is connected to a Summit 400, the `show ports configuration` command on the Summit X450 always reports SYM as flow control (PD3-34629550, PD3-19190526).

Configuration Port Auto-Polarity

On a Summit X450 switch, the configuration port auto-polarity on/off does not apply to the combo port (PD3-34629778, PD3-24485732).

ACL

Default Egress Deny-All ACL Does not Block Multicast Traffic

If you run the `clear ipmc fdb` command, initially some multicast packets are forwarded in slow path. Those slow path forwarded multicast packets are being denied by ACL (PD3-88458683).

ACL Cannot Deny vMAN Traffic with Unknown Destination Address

When an egress ACL is used to deny vMAN traffic with unknown unicast, multicast, and broadcast destination addresses, the egress ACL cannot deny the traffic (PD3-76416480).

Creating Dynamic ACLs Using Operands Results in an Error

Creating dynamic ACLs using the operands “<” or “<=” results in an error. Use “lt” and “lte” instead (PD3-94304401, PD3-42872248).

Summit X450a and Summit X450e series switches and BlackDiamond 8800 a-series and e-series Modules: Boot Time and Timing for Applying ACLs

Summit X450a and Summit X450e series switches and BlackDiamond 8800 a-series and e-series modules provide more powerful ACL capabilities. Because of this, the amount and complexity of ACL rules will naturally impact the time needed to process and apply the ACL rules to the switch. This will also impact switch bootup time. Access Control List limitations fall into two areas: physical and virtual.

Physical Limits—Summit X450a and Summit X450e series switches: The per-VLAN, wildcard (port any), and single-port access list installation limitations are 1024 rules for the Summit X450e and 2048 rules for the Summit X450a.

Physical Limits—BlackDiamond 8800 a-series and e-series modules: The per-VLAN, wildcard (port any), and single-port access list installation limitations are 1024 rules for the e-series modules, and 2048 rules for the a-series modules.

Extreme Networks recommends that you configure ACLs as per-VLAN, wildcard, or single-port. If either of the following is true, you will have to configure ACLs with multi-port lists:

- Your application requires that ports do not have a homogeneous ACL policy.
- When BlackDiamond 8800 original series modules are operational in the same chassis, it may be necessary to configure ACLs to specific port-lists instead of as wildcard or per-VLAN. This is because the original series modules have smaller physical limits.

Virtual Limits—Summit X450a and Summit X450e series switches: When configuring a multi-port ACL, use the following guideline. The total ACL count (as calculated by ACL rules times ports applied to) should not exceed 48,000 total ACL rules.

For example, applying a 1,000 rule policy file to a 48 port multi-port list is supported ($1,000 \text{ rules} * 48 \text{ ports in the list} \leq 48,000$).

Virtual Limits—BlackDiamond 8800 a-series and e-series modules: When configuring a multi-port ACL, use the following guideline. For any a-series or e-series blade in the system, its total ACL count (as calculated by ACL rules times ports applied to) should not exceed 48,000 total ACL rules.

For example, applying a 1,000 rule policy file to a 48 port multi-port list on an a-series module on slot 1 and an e-series module in slot 2 is fine. Neither module exceeds the 48,000 total ACL rules.

Excessive boot times and CPU resource starvation can be seen with larger total rule counts. If your application requires additional capacity, contact Extreme Networks (PD3-77983510).

Adding Large Number of Dynamic ACLs as Priority First May Fail

During testing it was discovered that creating more than 370 dynamic ACLs, added as priority first, causes the switch to crash (PD3-79357521).

Only One Egress ACL per vMAN Currently Supported

Multiple egress vMAN ACL rules with identical IF-conditions but different egress ports cannot be distinguished. Packets are going to be forwarded based on only one of the applicable rules (PD3-56605924).

Changing the Name of a Rule but not its Conditions or Actions Causes an Error

Changing the name of a rule in an ACL policy but not its conditions or actions, and then performing a refresh, causes a "duplicate" error on BlackDiamond 8806, BlackDiamond 8810, and Summit X450 switches (PD3-56552466).

ACL Action replace-dscp Not Taking Effect when Traffic Egresses on a Second Switch

The ACL action `replace-dscp` is not taking effect when traffic egresses on a second switch. Traffic egressing on the same switch is working properly (PD3-58209747).

ACL actions mirror-cpu and log/log-raw not logging messages

The `show access-list dynamic counter` command output does not give the correct counters or log the correct packets (PD3-58200199, PD3-42447111).

Policy-Based Redirect Cannot Redirect Across Two Virtual Routers

Policy-based redirect works properly within one virtual router (tagged or untagged VLANs), however, if you try to redirect traffic to a VLAN that belongs to a virtual router other than the one sending ingress traffic, the redirect does not work (PD3-54549831).

ACL Ethernet SNAP Packets Cause the Wrong Dynamic ACL Counters to Increment

Configuring dynamic ACL Ethernet Subnetwork Access Protocol (SNAP) packets causes the wrong dynamic ACL counters to increment (PD3-58149031).

ACL ICMP Keyword for Timestamp is not Working

The keyword `icmp-type timestamp` when used in an ACL policy match condition does not work. Using the ICMP number code instead of the keyword works correctly (`icmp-type 13`) (PD3-55929951, PD3-41829516).

Modifying a Port Range in an ACL Rule May Cause an ACL Blackhole

Modifying the port range of an ACL rule may cause a temporary blackhole or packet leak while refreshing on a BlackDiamond 8806, BlackDiamond 8810, or Summit X450 switch. To avoid this, modify the port range ensuring the new range does not overlap the old range. Alternatively, to avoid the packet leak, enable blackholing (PD3-51329744).

Cannot Save Policy File Using a Different Name

When you edit `tcpDestPort.pol` using the VI editor and save it with a different filename, the new file is not applied (PD3-27536111).

MAC and IP MAC Entries Allowed in the Same IPv6 ACL Rule Entry

MAC and IP MAC entries are being allowed in the same IPv6 ACL rule entry. L2 and L3/L4 rules should not be allowed in one entry; this should fail the grammar check but does not (PD3-28320337).

Invalid Encapsulate Value for IPv6

In IPv6, the encapsulate value is `next header`, which is not currently a valid attribute (PD3-28320363).

ACL mirror-cpu and log Feature

When using ACL “mirror-cpu” and “log” actions on a Summit X450 or a BlackDiamond 8810 switch, only layer-3 and layer-4 match conditions will cause packets to be logged when packets are routed

through the switch. Additionally, only port-based and wildcard ACLs generate a log for routed packets. Layer-2 switched packets are not subject to these limitations.

Peer IP Address is Missing in BGP Traps

BGP traps transmitted from a BlackDiamond or Summit X450 switch are missing the peer IP addresses (PD3-41952658).

CLEAR-Flow

“show clear-flow vlan” Command Displays Invalid Threshold Type

If you use the `show clear-flow vlan <vlan name>` command, RL may appear in the output as a threshold type. RL is an invalid threshold type and should not appear in the output (PD3-95652911, PD3-95652994).

CLEAR-Flow is Not Supported on Summit X450 and BlackDiamond 8800

CLEAR-Flow is not supported on Summit X450 and BlackDiamond 8800 switches (PD3-60258721).

CLEAR-Flow Does not Require a Space around Operators

CLEAR-Flow does not mandate a space around operators. This should be required (PD3-57208227, PD3-71744964, PD3-73126821).

CLEAR-Flow is Only Supported on BlackDiamond 10808 and BlackDiamond 12804 Systems

A syntax error is not displayed when a policy file is configured using CLEAR-Flow rules on BlackDiamond 8810, BlackDiamond 8806, and Summit X450 switches. The rule is silently ignored (PD3-16311713).

CLI

Load Script Unable to Process Banner Configuration

The `load script` command is unable to process banner configuration (PD3-125018491).

“show configuration” Command Output Includes Invalid Switch Prompt

The `show configuration` command output includes the invalid switch prompt `configure vr VR-Default add ports 1:1-2:48, 4:1-10:48` (PD3-77316227).

Timezone/DST Name Truncates at Seven Characters

When configuring an optional name for the timezone/DST on the Summit X450 family of switches, the timezone name truncates at seven characters. The system default is six characters (PD3-71725881).

“show odometers” Command Does not Display PSUCTRL Service Days

The `show odometers` command does not display PSUCTRL service days. It only displays 0 service days (PD3-67968832).

RX Align Counter is not Incremented

For the incoming traffic with alignment errors, the "RX Align" counter in the output of the `show ports <Port Number> rxerrors` command is not incremented. Instead the "RX CRC" counter is incremented (PD3-57182431).

“enable ipforwarding fast-direct-broadcast | ignore-broadcast” Command is Not Supported

The CLI command `enable ipforwarding fast-direct-broadcast | ignore-broadcast` is not supported in ExtremeXOS (PD3-61996631).

“upload configuration” Command Contains RIP Configuration Commands

The `upload configuration` CLI command contains RIP configuration commands in spite of there not being a RIP VLAN (PD3-63858286).

“upload configuration” Command Generating Invalid CLI

While uploading a configuration using the `upload configuration` command, remove the following invalid CLI:

- On a Summit X450 switch: `configure slot 1 module SummitX450-24t` (PD3-63772664)
- `configure mstp region 00049620ad93`
`create stpd s0` (PD3-63875328)
- `configure ospf vlan com` (PD3-63858254)
- `configure firmware` (PD3-63858238)

“show ports mgmt utilization” CLI Command Does not Show any Statistics

The `show ports mgmt utilization` command does not show any statistics. The command output is all zeros (PD3-40450253).

Control Protocols

Switches Configured for VRRP can Experience State Changes

If you have the following VRRP configuration on two neighboring and connected switches, where one switch is the VRRP master and one is the backup:

- VRRP supported VLANs-128
- VRRP advertisement interval-100 milliseconds
- Number of tracked ping entries-1,024 (8 track-pings per instance)
- Frequency of tracking ping entries-3 seconds
- Number of times before the entry is considered failing-3 misses

You may experience multiple VRRP state changes between the two switches.

Workaround. To prevent this from occurring, use the `configure vrrp vlan vrid advertisement-interval` command to change the VRRP advertisement interval to 1 second or 100 milliseconds, with frequency interval 3 seconds, retry three times when using two track-pings per instance with 128 instances configured. Or, with frequency interval 9 seconds, retry three times, when using four track-pings per instance with 128 instances configured.

(PD3-95580434)

When a Port Link is Down or Disabled, UPM Should Register a Device-Undetect

When an LLDP enabled port link is down or disabled, Universal Port Manager may take up to 30 seconds to register a UPM device-undetected event (PD3-94406464).

Convergence Time May Increase After Removing Root Bridge from dot1s Network

Convergence time may increase (approximately 90 seconds) when a root bridge is removed from a dot1s network (PD3-79194922).

Multiple BPDUs Sent From Root Port

When the configured link type is broadcast, multiple BPDUs are sent from the Root port every two seconds, even after the topology converges (PD3-78170111).

CIST Ports Link-Type Configured as Point-to-Point Lost When Configuration is Uploaded and Downloaded

When creating a CIST domain and then configuring the link-type as point-to-point for CIST, the link-type configuration is lost when the uploaded configuration is downloaded (PD3-75421071).

Summit X450a May Briefly Lose Data During a Failover

Large routing table updates affect the convergence time for EAPS and VRRP failovers (PD3-77283998).

MSM Failover on ESRP Slave Running IGMP Causes Packet Loss

If you are running MSM failover on a BlackDiamond 8800, when the backup MSM boots up and is synchronized with the primary MSM, port A is unblocked and sends out an IGMP report to group 224.0.0.2 and 224.0.0.22, with ESRP VMAV as source mac. Since IGMP is enabled on those 500 ESRP vlans This causes the VMAV to be re-learned on a BlackDiamond 10808 and the traffic is redirected to a BlackDiamond 8800 (PD3-67713552).

STP Blocks CFM Packets

Connectivity Fault Management (CFM) packets are not received on ports blocked by STP, EAPS, and ESRP (PD3-60905520).

Device Management

Specifying Port Numbers Does not Clear Number of Shared Ports from FDB Table

Specifying port numbers in the `clear fdb` command does not clear the number of shared port entries in the FDB table (PD3-134477165).

WAN-PHY Trace Path String Cannot be Longer than 16 Characters

Configuring a WAN-PHY trace path with a string longer than 16 characters causes the switch to reboot after running the `show ports <wan-phy port no> wan-phy configuration` command (PD3-133764591).

DOS Console Window Does not Wait for User Input

The DOS console window does not wait for user input after executing the `unconfigure switch all` command (PD3-84049005).

ZX Mini-GBIC Appears as an LX Mini-GBIC on the Summit X450e-48p Switch

When installing a ZX mini-GBIC into a mini-GBIC port on the SummitX450e-48p switch, the switch displays it as an LX mini-GBIC (PD3-95643404).

Extraneous Errors Displayed when Loading a Non-Existent Variable

When loading a non-existent variable, the switch displays output similar to the following:

```
Error: Failed to import variable port3 from key ports. Variable does not exist while
executing
"exsh_var import $args(<keyname>) $temp" ("for" body line 3)
invoked from within "for {set i 9} {$i < $argc} {incr i 2}
{set temp [lindex $argv $i] exsh_var import $args(<keyname>) $temp}"
```

You should only see an error similar to the following:

```
Variable does not exist.
```

You can safely disregard the other output (PD3-95714861).

Do not Use “configure-sys-recovery level slot” Command on MSMs

Do not use the `configure-sys-recovery level slot shutdown` command on an MSM slot. This can result in I/O modules that remain active after a hardware failure, even if the modules are configured to shutdown (PD3-77979260).

“show configuration” Command Output Shows Wrong Information

The output for the `show configuration` command includes some default configuration commands that are not available for user configuration (PD3-77949095).

Diagnostics

Management Port Reported as Down in Shutdown State

When Summit X450a and X450e series switch is in the shutdown state, all ports must be down with the exception of the management port. However, the management port is also down (PD3-87341149).

sys-health-check Configurations are not Stored in Uploaded Configurations

System health check related configurations are not stored in uploaded configurations (PD3-74554921).

EAPS

EAPS Loop Created when an EAPS Shared Port Partner Comes Up

An EAPS loop is created when an EAPS shared port partner comes up after a reboot (PD3-149806981).

.Changing Shared Port Link ID When the Shared Link is Down

Changing the EAPS shared port link ID of a partner/controller pair while there is a failure in the EAPS network is not recommended and may cause a loop in the network (PD3-96983520).

Traffic Loss Occurs When a Shared Link Comes Up

When traffic is running between shared links, FDB entries are incorrectly learned on BlackDiamond 10808 and BlackDiamond 12804 switches. Traffic loss occurs until the incorrectly learned FDB entries age out (PD3-104885349).

If Multiple Shared Links are Down, a Loop is Created

In a specific EAPS topology, if multiple shared links are down, a loop is created (PD3-97153785).

Number of EAPS Domains Supported by Advanced Edge License

Although it is possible to configure more than four EAPS domains on a switch with an Advanced Edge license, this is not supported (PD3-78599455).

Simultaneously Disabling Three Shared Port Links can Cause an EAPS Loop

Configurations having three shared links, where the shared link with the lowest ID is in the middle, the root blocker marks the segment as "blocking-down," but the ports are not in a blocked state.

To get out of the loop, restore the shared links. To avoid encountering this condition, insure that no more than two shared links become disabled (PD3-135517703, PD3-135517553, PD3-87003427, PD3-78960443, PD3-78302829).

EAPS Warning Messages are Displayed from VLAN Manager even after Turning Off Config-warnings

EAPS warning messages are displayed from the VLAN manager even after running the `configure eaps config-warnings off` command (PD3-95187020, PD3-72086161).

Disabling a Slot on a BlackDiamond 12804 Causes a Loop in EAPS Setup

Configuring two EAPS sharing links on a slot and disabling both sharing links at the same time causes a loop of approximately 1.5 seconds on a BlackDiamond 12804 (PD3-56877301).

EAPS with Load Sharing Enabled/Disabled Causes Control Packets to be Received on Port

Misconfigured EAPS control VLAN ports may not be detected, causing EAPS PDUs to be accepted into the system even though they were received on an incorrect port (PD3-54870537, PD3-45729158).

EAPS in Active Root Blocker State

When EAPS is in the Active Root Blocker state, that is, there are two more common links that are down, it is possible to have a disconnected network on some VLANs. The VLANs that are affected are the VLANs that do not span the entire network. This happens because EAPS forces blocking of VLANs to prevent a loop. EAPS does not check to see if a loop was going to happen in the first place, thereby causing a disconnected network for those VLANs (PD3-27767509, PD3-27536496).

ESRP

ESRP Slave Switch with Host Attach Ports does not have an ESRP Virtual MAC IP Address

On a Summit X450a series switch, an ESRP slave with host attach ports does not have an ESRP virtual MAC IP address in the FDB table (PD3-143386741).

vMan Switches that act as ESRP-aware Cannot Forward Tagged ESRP Control Packets

vMan switches that act as ESRP-aware cannot forward tagged ESRP control packets, resulting in an ESRP dual master situation. If the ESRP ports are used as untagged ports, this issue does not occur (PD3-130145823).

MSM-Failover Causes ESRP Master Switch to Become ESRP Secondary Switch

An MSM failover on a BlackDiamond 10808 that is operating as an ESRP master may trigger an ESRP mastership change, causing the switch to become an ESRP slave (PD3-83773893).

MSM Failover from ESRP Master Causes an FDB Flush on new Master

An MSM failover from an ESRP master causes an FDB flush on the new master during the pre-master to master transition (PD3-103123831).

VLAN Tracking Fails after an MSM Failover

On a BlackDiamond 8810, when an ESRP domain is configured with VLAN tracking, ESRP transitions to the SLAVE state when the tracked VLAN goes down (that is, all the VLANs ports go down). After an MSM failover, the ESRP domain transitions to the master state, even though it still shows the tracked VLAN is down (PD3-61629918).

Disabling a Shared Port Makes the ESRP Port Restart configuration disappears

Disabling a shared port results in the ESRP port restarting and the configuration disappearing (PD3-52741820).

Potential Problem with Graceful Disable of ESRP

Graceful disable of ESRP may cause a momentary loop in the network (PD3-26330059, PD3-14890821).

Summit X450 Does Not Show all ESRP-aware Masters

After configuring several ESRP domains on a Summit X450 without enabling them, the `show esrp` command only shows the first domains ESRP-aware master MAC address; it does not contain ESRP-aware information in the summary display. If you issue the `show esrp individual domain` command, ESRP-aware information is displayed (PD3-35920481).

IP Routing Protocols

Extreme Devices do not Support the PIM Prune Timer Option

Extreme devices do not send the PIM prune timer option in Hello packets, and ignore it when it is received. This behavior may lead to an increase in multicast traffic in the network (PD3-133674452).

“configure ipmroute” is not Applied Correctly on BlackDiamond 10808

Configuring static IP multicast routes is not triggering a prune or join from a BlackDiamond 10808 with PIM enabled (PD3-132870161).

IPv6 Multicast Flooding is Occurring in Software

IPv6 multicast forwarding is performed in software on all platforms (PD3-90764853).

ICMP Packets are not Answered Correctly

The switch does not answer back IPv6 ICMP packets correctly (PD3-100339658).

IGMP Memberships are Flushed if STP Link Goes Down

When an STP link goes down, IGMP memberships are flushed, resulting in a drop in traffic (PD3-90875982).

Packets Switched to SPT when TX Rate is Less than the SPT Threshold

When packets are sent as IP multicast data at 10Mbps, the packets are switched from RPT to SPT (PD3-92235491).

MVR not Sending Periodic IGMP Reports

MVR is not sending periodic IGMP reports if the MVR VLAN is an L2 VLAN and configured static router (PD3-90712545).

IGMPv3 Report Record Type "5" Message Does Not Work Correctly

IGMPv3 Report Record type "5" does not work as expected when sent after a type "2" or a type "4" message (PD3-79383551).

unconfigure pim Command Removes SSM Configuration

The `unconfigure pim` command removes an SSM configuration but leaves the SM configuration unchanged (PD3-73130391).

IPv4 Capability Must be Configured for BGP Restart to Work Properly

For BGP graceful restart to work with third party operating systems, IPv4 capability may have to be configured in ExtremeXOS (PD3-52605136).

show pim Command Should Return an Error Message When Protocol Not Added to User VR

When a protocol PIM is not added to a user VR, the switch does not return an error message when you run the `show pim` command from the user VR (PD3-40476272, PD3-28467998).

IPv4 Unicast

show platform ipv4Fib Command does not Support CLI Paging

The `show platform ipv4Fib` command does not support CLI paging. When 5,000 OSPF routes are learned, this command will display about 15 minutes of output that cannot be interrupted by the user (PD3-91421737).

IPv6 Unicast

Packets Forwarded Through Tunnels Do Not Use Fast Path

On the Summit X450a and X450e switches, IPv6 packets for IPv6-in-IPv4 and 6-to-4 tunnels are forwarded in software. Normal IPv6 forwarding, for routes up to a 64 bit mask, are forwarded at line rate (PD3-79041026).

Neighbor Discovery Cache Allows Addition of Static Entry for Existing Address

The switch will allow you to add a Neighbor Discovery Cache entry, even if that entry matches an existing VLAN IP address. No error or warning message will be displayed (PD3-78254331).

IPv6 FIB and Adjacency Entries Cleared When Duplicate Address Detected

When a duplicate IPv6 address is detected (DAD), all the IPv6 FIB and adjacency entries are cleared. The entries are not rediscovered, even when the duplicate address is removed (PD3-78254454).

ICMPv6 Destination Unreachable Message Not Generated

Using a routing extension to send a packet beyond the scope of the packet's destination, the DUT does not generate an ICMPv6 destination unreachable code 2 (PD3-40462332, PD3-26580819).

Mirroring

Mirroring Port Should Not be Allowed in Load Sharing

If you create a load sharing group (trunk), then enable mirroring to a port, the software will allow you to add the mirroring port to the load sharing group (PD3-79867211).

Enabling Load Sharing on a Mirrored Port

Enabling load sharing on a port that is being mirrored causes the mirroring to stop (PD3-28378521).

MPLS

Router not able to Forward Multicast Traffic to its VPLS Peers

A timing problem exists that can result in a router not being able to forward multicast traffic to its VPLS peers. The problem is triggered by rebooting, disabling and then enabling MPLS, or disabling and then enabling VPLS.

Workaround. Disable and enable each VPLS instance individually.

(PD3-106670928)

Router Address may Inadvertently be Purged from the OSPF Database

When an OSPF database exchange occurs, if the LSID for the OSPF router address has changed and the neighbor's version must be flushed (for example, after a reboot), the router address may inadvertently be purged from the CSPF database. This usually results in an LSP error similar to Invalid Source Address or No Outgoing Interface Found in the output of the `show mpls rsvp-te lsp detail` command. As a result, RSVP-TE LSPs may fail to come up until an OSPF refresh occurs (default: 30 minutes). A similar problem may occur that causes the flush and incorrect purge in the CSPF database to occur on the neighbor. In this case, the error reported by the `show mpls rsvp-te lsp detail` command is No route available toward destination. Note that No route available toward destination is a common error and may occur for other reasons as well.

Workaround. Disable RSVP-TE or OSPF on one or both routers.

(PD3-104046299)

show mpls rsvp-te lsp detail Command may not Show Error Condition

If the transmit bandwidth between two RSVP-TE neighbors is sufficient for a given LSP, but the receive bandwidth is not, the LSP does not come up. The reason for the error is not displayed in the `show mpls rsvp-te lsp detail` output (PD3-99318269).

Egress LSPs using Advertised Implicit NULL Labels are not Displayed

The `show mpls label`, `show mpls rsvp-te label`, and `show mpls rsvp-te lsp` command output currently does not display egress LSPs using advertised implicit NULL labels (PD3-92653036).

Changing Ethertype on VPLS Service vMAN Causes Traffic to Stop Forwarding

Changing the Ethernet type on a VPLS service vMAN causes the device to stop forwarding traffic (PD3-128184768).

Configuring a VPLS Pseudo Wire ID of 0

Configuring a VPLS pseudo wire ID of 0 should not be allowed.

Workaround. Do not use an ID of 0.

(PD3-127944432)

MPLS does not Handle Restarting OSPF

If OSPF is restarted, MPLS must send data to OSPF after it restarts, which MPLS is not currently doing.

Workaround. Restart OSPF and then restart MPLS.

(PD3-125508231)

Data Corruption and Subsequent Crash may Occur when Enabling and Disabling RSVP-TE

When numerous RSVP-TE LSPs are configured, enabling and quickly disabling RSVP-TE may cause data corruption and eventually a system crash (PD3-125485371).

Disabling and Enabling MPLS may Result in LDP Sessions Staying in a Non-Existent State

Under certain circumstances, disabling and enabling MPLS causes LDP sessions to stay in a non-existent state. This only occurs if there are two or more adjacencies.

Workaround. Disable and enable LDP on the affected interfaces and disable and enable any VPLSs to that peer.

(PD3-124219816)

SNMP Trap is not Generated for Blackholed FDB Entries

An SNMP trap should be generated for each blackholed FDB entry after reaching the MAC learning limit for a VPLS peer. The logs show that the limit is reached and entries are blackholed, but no SNMP trap is generated (PD3-123285381).

Dynamically Changing IP MTU can result in VPLS Sessions not Coming Up

If an IP MTU is changed while a VPLS session is operationally up, the VPLS session goes down and fails to come back up.

Workaround. Disable and enable MPLS at both VPLS peers.

(PD3-121740899)

Blackhole FDB Entries Incorrectly Adding when using VPLS MAC Limiting Feature

When using VPLS MAC limiting, extra blackhole entries may be added to the FDB for no reason (PD3-121230737).

VPLS Limit Learning Causes FDB Entries Learned over VPLS to be Blackholed

VPLS incorrectly writes a value of 0 to configuration files for unlimited learning. When 0 is read in from the configuration file, addresses are not learned, they are blackholed.

Workaround. If necessary, reconfigure VPLS limit learning.

(PD3-121206111)

Log Messages may be Generated during LSP Ping

Link flapping and other similar issues may cause an LSP ping to generate a log similar to:

```
01/19/2007 01:53:04.22 <Error:MPLS.Ping.Error> MSM-A: Couldn't find lsp to fec x1e0.
```

This log reflects link instability affecting the availability of LSPs and can be ignored (PD3-121098111).

Frames Exiting a Pseudo Wire are not Mirrored

Frames exiting a pseudo wire are not mirrored when ingress mirroring is activated (PD3-120757801).

When Disabling MPLS L2 VPN Log Messages may be Generated

When disabling MPLS with a large number of VPLSs, L2VPN.fecSendFail log messages may be generated (PD3-118893434).

Enabling or Disabling PHP on a VLAN does not Work if MPLS is Enabled

Enabling or disabling penultimate hop popping on a VLAN does not work if MPLS is enabled (PD3-117148339).

“show mpls ldp peer” Command does not Show Peer if Peer is Using an Interface Label Space

The `show mpls ldp peer <lsp-id>` command does not show a peer if the peer is using an interface label space. The `show mpls ldp peer` command does work (PD3-117124291).

Disabling MPLS may Cause MPLS HAL Log Messages

Disabling MPLS may cause MPLS HAL log messages similar to the following:

```
12/21/2006 07:28:29.84 <Error:MPLS.Error> MSM-A: mplsHalDeleteIlm: Cannot find ILM 14 (label 10) to delete.
```

These logs may indicate a more serious problem that requires a reboot to correct.

Workaround: Disable and enable LDP.

:(PD3-115971486)

Dynamically Configuring LDP to Advertise RIP Routes does not Work

If LDP is not configured to advertise RIP routes, and the configuration is changed such that LDP should advertise RIP routes, the actual RIP route advertisement is not affected.

Workaround. Disable and enable LDP.

(PD3-115936761)

VPLS Session Remains UP even if Configured to use a DOWN named LSP

A VPLS can be configured to use only a specific named LSP. If the VPLS is UP when the configuration is changed to use a named LSP, but the named LSP is DOWN, the VPLS should go down because the transport LSP is not available

Workaround. Manually disable and enable the VPLS.

(PD3-115548009)

Changing a VLAN from Tagged to Untagged may Result in LDP not Advertising a Label for that VLAN

LDP may stop advertising a label for a VLAN when the VLAN and ports that are part of the VLAN are changed from tagged to untagged or vice versa (PD3-114996515).

nettx Logs When Trying to Forward 802.1Q Tagged Packets through VPLS

Port flapping, and other problems, can cause logs similar to the following when 802.1Q tagged packets are software forwarded for a VPLS service VLAN:

```
12/15/2006 08:11:40.67 <Error:Kern.Error> MSM-A: nettx_vpls_transmit.(987) VPLS -
problems determining .1q tag for encapsulated packet.
```

The logs are the result of other problems such as port flapping and will no longer appear when the other problems are corrected (PD3-114261166).

Globally Enabling IP Forwarding on all VLANs Incorrectly Results in IP Forwarding being Enabled on VPLS Service VLANs

IP forwarding cannot be enabled on VPLS service VLANs. However, if IP forwarding is globally enabled for all VLANs using the `enable ipforwarding` command, the service VLANs will have IP forwarding enabled (PD3-112398430).

Explicit NULL Labels are Treated as Implicit NULL Labels

When a router receives an explicit NULL label, it is incorrectly treated as an implicit NULL label, so rather than sending label 0, no label is sent (PD3-111544904).

VPLS and LSP Statistics—Do Not Include Counters from Ports Mapped to Backup MSM

On a BlackDiamond 10808, the counters from ports mapped to the backup MSM are not included in the VPLS and LSP output for received bytes and packets shown in the command output for the `show mpls ldp lsp detail`, `show mpls rsvp-te lsp`, and `show vpls detail` commands (PD3-111544750).

The “clear counters” Command may Result in MPLS HAL Log Messages

The `clear counters` command, or variations of the command, may result in MPLS HAL log messages similar to:

```
01/30/2007 13:09:40.87 <Error:HAL.MPLS.Error> MSM-A: gnsilm entry not found for
ilmstance 30.
```

These log messages can be ignored (PD3-110196861).

Switch Experiences High Packet Loss

The switch experiences high packet loss when issuing the `run msm-failover` command numerous times on the ingress/egress switch (PD3-125916129).

After Issuing run msm-failover Command Traffic Does not Completely Recover

After running the `run msm-failover` command, traffic does not completely recover in both directions (PD3-118425312).

Traffic Rate Drops over the VPLS Pseudo Wire after an MSM Failover

The traffic rate drops over the VPLS pseudo wire after an MSM failover and the traffic rate continues to flap (PD3-109003470).

LDP Sessions Flap Because Hello Packets are not Periodically Sent after a Failover

LDP sessions flap between operational and non-existent because of missing hello packets after an MSM failover (PD3-125916164).

LDP Path Vector Limit is not Working

LDP path vector loop detection may not perform as expected. For example, the LSR can advertise and propagate path vector TLVs, but will not reject FECs whose path vector value exceeds the configured path vector limit (PD3-116640291).

LDP Path Vector Loop Detection may only Include Nexthop Path Vector LSR-ID

When enabling the LDP loop detection feature, the path vector TLVs LSR-IDs are not updated.

Workaround: Disable and enable MPLS.

(PD3-116409584)

LDP Hop Count Loop Detection may not Work Properly

LDP hop count loop detection may not work properly on transit LSRs.

Workaround. Disable and enable MPLS.

(PD3-116387966)

Packets with Router Alert Label (0x00001) are not being Forwarded

If either an egress or a transit LSP traverses the system, and an MPLS labelled packet containing a router alert label is received, that packet is not forwarded (PD3-93218551).

VLANs Configured as Protocol “any” Should be Added to MPLS

Only VLANs configured as protocol `any` should be added to MPLS (PD3-93069318).

LDP Session does not Exit NonExistent State

LDP sessions may fail to transition from the NonExistent state when multiple link adjacencies exist.

Workaround. Run the `disable and enable mpls protocol ldp` command.

(PD3-108133805)

ExtremeXOS does not Send back ICMP Responses for Traceroute through Non-Pipe Mode LSPs

When a traceroute is performed by setting the MPLS TTL to the IP TTL, ExtremeXOS does not correctly send back an ICMP response. The result is "*" characters in the traceroute for the routers that timed out. If a route is available, ExtremeXOS should attempt to send back an ICMP response (PD3-104731701).

LDP Should Not Advertise Certain Label Mappings

LDP should not advertise a label mapping for a direct VLAN that does not have IP forwarding enabled (PD3-93630853).

Labels for Static and RIP Routes not Advertised

LDP advertises label mappings for static and RIP routes based on the setting of LDP options. When `configure mpls ldp advertise static` and `configure mpls ldp advertise rip` commands are

issued while MPLS is enabled, label mappings may not be advertised as expected. To insure proper operation, MPLS should be disabled prior to issuing these commands (PD3-99398361)

MSM Failovers Displays Numerous Errors on Switch Console

With 100 VPLS peers configured, and while sending traffic of incrementing SRC_MACs, numerous error messages are displayed on the console (PD3-98490936).

EXP Field Examination and Replacement not Working

Classifying MPLS packets based on EXP field examination, and EXP field replacement are not supported (PD3-97185211).

Sending LDP Labels and Stopping Transmission Causes Error

Some LDP ECMP topologies may cause the following error message to be logged when label switched paths (LSPs) are released:

```
RTR_E_BD12K.22 # show log

10/04/2006 16:21:46.56 <Erro:MPLS.Error> MSM-A: mplsHalDeleteIlm: Cannot find ILM 574
(label 2e7) to delete

10/04/2006 16:21:46.55 <Erro:MPLS.Error> MSM-A: mplsHalDeleteIlm: Cannot find ILM 598
(label 30d) to delete

10/04/2006 16:21:46.55 <Erro:MPLS.Error> MSM-A: mplsHalDeleteIlm: Cannot find ILM 601
(label 314) to delete

10/04/2006 16:21:46.55 <Erro:MPLS.Error> MSM-A:
```

(PD3-100051127)

Pings and Traceroutes May not be Sent Using an LSP Even Though an LSP Next Hop is Available

The ExtremeXOS route table and kernel route table show that an LSP next hop for a specific route is available. However, when `ping` or `traceroute` commands are issued for a destination reached by the route, the LSP next hop may not be used (PD3-88153931).

LDP traffic needs to be prioritized

Sending a 100 Mbps data stream with a destination address of `broadcast` on a Virtual Private LAN Service (VPLS), causes the Label Distribution Protocol (LDP) to flap. OSPF remains open, which indicates that the LDP TOS bits may not be set to prioritize LDP control frames (PD3-76640281).

Multicast

Multicast Groups Continue to Age Out

After the host timeout of 260 seconds, multicast groups should be deleted. However, the age continues to increase and the groups are never deleted (PD3-101466421).

No Entry for pimInterfaceTable When Configuring PIM

When configuring PIM, there is no entry for pimInterfaceTable (PD3-58264172).

At Line Rates, a Large Percentage of IP Multicast Packets Sent to PIM RP Will be Dropped

When sending 10808 IP multicast packets at the line rate into DUT, only a few packets are processed and sent to the RP, causing PIM caches not to be created on the RP. If traffic is sent twice, or continuously, the PIM cache entries will be created on the RP after the initial packet loss. This applies to BlackDiamond 8810 and Summit X450 switches only (PD3-28410081).

show pim Command Only Counts Null-Registers

The output of the `show pim` command displays the cumulative counter for the PIM register in/out and the register-stop in/out. When the ExtremeXOS switch is a first-hop router, it sends out the real register first. After a particular mroute has been established, PIM then periodically sends the null-register. The "Register out" field does not count real registers; it only counts null-registers (PD3-16451411).

Multi-access VLANs with Two Upstream Neighbors Drop Assertion Messages

A timing issue with CPU packets is causing assertion messages from upstream routers to be dropped. Traffic can be disrupted for up to 210 seconds if the best route to the source network is equal from more than one upstream neighbor. If there is a unique best to the source, traffic is not disrupted.

Workaround: Configure a receiver on the multi-access VLAN so the assertion winner does not go into a temporary pruned state. Change the link cost so that there is a unique best route to the source network.

(PD3-6251082)

Network Login

“show netlogin” Command does not Display IP Address of 802.1X Supplicant Authenticated on Tagged Port

When an 802.1X supplicant authenticates on a tagged port, the `show netlogin` command displays 0.0.0.0 for the supplicant even after the supplicant obtains an IP address (PD3-99123566).

Network Login "move-fail-action" not Working Properly

When a move-fail-action is configured as authenticate and a client tries to get authenticated on a tagged VLAN on a port that already exists in the same VLAN as untagged, the move fails. Therefore, the client has to be authenticated in the VLAN as untagged, but the client currently remains unauthenticated (PD3-99061252).

Network Login Syslog Error Message

When Network Login is configured, the syslog should not display the following message when rebooting a Summit X450.

```
05/18/2006 15:31:10.62 <Noti:HAL.Port.Notice> aspenCardPortEnableNetlogin(1:11, 255)
- Netlogin is already enabled.
05/18/2006 15:31:10.62 <Noti:HAL.Port.Notice> aspenCardPortEnableNetlogin(1:10, 255)
- Netlogin is already enabled.
```

(PD3-76900229)

Network Login Client Needs to be Reauthenticated After flush-fdb

If EAPS and STP are enabled together a topology-change-notification is received by STP and can cause EAPS to flush all FDB entries on the switch. This causes Network Login clients to become unauthenticated and Web login clients, in particular, need to login again (PD3-62154121).

Guest VLAN Functionality does not Work Correctly with Multiple Supplicants

When multiple supplicants are not responding to EAPOL with 802.1x guest VLAN enabled, both supplicants are moved to and authenticated in the guest VLAN. If one of the supplicants is successfully authenticated, it still remains in the guest VLAN (in both ISP mode and Campus mode). If the authenticated supplicant then sends an EAPOL stop, all supplicants in the guest VLAN on that port are unauthenticated (PD3-45960179).

Web-based Network Login Authentication through Network Login Local User Database

When web-based Network Login authenticates through the Network Login local user database, the following web Network Login features are not applied:

- Default-Redirect-Page
- Logout-privilege,
- Netlogin Session-Refresh

(PD3-28603401)

Network Services

Ingress ACL "source-address 0.0.0.0/0" Matches Every Protocol Instead of IP Packets

On the BlackDiamond 10808 switch, BlackDiamond 12800 series switches, and the Summit X450 switch, the ingress ACL match condition "source-address 0.0.0.0/0" matches only to IP packets. However, for

Summit X450a and X450e series switch, the ingress ACL match condition matches not only IP packets but also every protocol (PD3-131866132).

Changing Traffic Queue Mode to Bandwidth Mode Requires Two Reboots

The `unconfigure switch all` command resets the configured traffic mode. Changing the traffic mode requires another switch reboot (PD3-100302218).

UPM Profiles Fail to Load

UPM profiles fail to load due to a line ending with the `>` operand (PD3-99950334).

Disabling Sharing fills Console with Warning Messages

After issuing the `disable sharing` command for an LACP trunk, the following warning message fill the BlackDiamond 8800 console:

```
Warning: Any STP related config on the master port is lost.
Warning: Any STP related config on the master port is lost.
Warning: Any STP related config on the master port is lost.
Warning: Any STP related config on the master port is lost.
```

(PD3-104054783)

Configurations Using VR-Mgmt Interface as RADIUS Client IP Do Not Load

Configurations using a VR-Mgmt interface as a RADIUS client IP may not load at boot-up. However, using an interface in VR-Default will load correctly (PD3-93829391).

show ipstats ipv6 tunnel Command Shows All IPv6 Statistics

The output of the `show ipstats ipv6 tunnel <tunnel-name>` command shows all IPv6 statistics, rather than just the statistics for the specified tunnel (PD3-77902212).

ARP Refresh Works Incorrectly When Default Value is Changed

ARP refresh works correctly when set to the default 20 minute timeout value. However, when the timeout value is reduced to two minutes, the entries age out without refreshing (PD3-78350716).

IPv6 Configuration Changes Generate Error Messages

IPv6 configuration changes, such as `clear neighbor-discovery cache ipv6`, or unconfiguring the IPv6 addresses on a VLAN, generate the following warning messages, which can be ignored.

```
05/23/2006 02:32:51.52 <Warn:netTool.routeradv.noVlanIfState> IP6 Router
Advertisement could not locate the configuration for vlan instance 1000050
05/23/2006 02:25:24.52 <Warn:netTool.routeradv.noVlanIfState> Previous message
repeated 2 additional times in the last 447 second(s)
```

(PD3-77236566)

Enabled MLD Switches do not Reject Other Group Addresses

The switch does not reject MLD report messages even if the IPv6 destination address is not the same as in the ICMPv6 group field (PD3-74553139).

Hop-Limit in IPv6 Header is Ignored for Inbound MLD Packets

An MLD packet with a hop-limit of 2 or more in the IPv6 header is not rejected by the MLD module (PD3-74553139).

Telnet Requests Sent from MSM-A to MSM-B Causes MSM-A to Fail

Telnet requests sent from MSM A to MSM B causes MSM A to fail and subsequent logging through the console into MSM results in a page fault (PD3-78278111).

Duplicate VLAN Tags will Cause Broadcast Packet to Drop

An SVLAN tag can be duplicated with other SVLAN tags as long as the ports on each SVLAN are not overlapped. The SVLAN tags cannot be the same as other regular VLAN or vMAN tags (PD3-65041471).

Creating Tagged vMANs and VLANs Using the Same Ports Sends Control Packets vMAN EtherType (0x88a8)

If you create a tagged vMAN and assign two ports and then create a tagged VLAN using the same two ports, the egress port for the control packets sends the packets with vMAN EtherType (0x88a8) instead of VLAN EtherType (PD3-63847461).

Ingress Rate Limiting and Egress Rate Limiting are Mapping to Multiple Ports

Configuring an ingress traffic queue and an egress traffic queue association to multiple ports in sequential order generates the following error:

```
Egress queue already associated to this ingress queue
Configuration failed on backup MSM, command execution aborted!
```

(PD3-67431351)

vMAN ID ACL Translations May Fail with Transmit Errors

Creating two sets of vMAN ACLs with 4000 entries each and performing a vMAN ID translation on each ACL may generate the following error:

```
.....03/15/2006 17:57:28.84 <Info:pm.config.openingFile> MSM-B: Loading policy RLL20k
from file /config/RLL20k.pol
...03/15/2006 17:57:32.46 <Info:pm.config.loaded> MSM-B: Loaded Policy: RLL20k number
of entries 4002
.....Error in alloc txmi txmi 0x9f2 txmdi 0xffffffff
Error in alloc txmi txmi 0x9f4 txmdi 0xffffffff
Error in alloc txmi txmi 0x1102 txmdi 0xffffffff
Error in alloc txmi txmi 0x9f6 txmdi 0xffffffff
Error in alloc txmi txmi 0x9f8 txmdi 0xffffffff
```

(PD3-67727590)

Checkpointing May Fail When Saving or Rebooting More than 4000 Traffic Queues

After creating 4000 traffic queues each and defining corresponding ACLs for each queue, saving and rebooting the switch may cause checkpointing to fail in the backup MSM with display the following error.

```
03/17/2006 15:07:42.64 <Info:HAL.Card.Info> MSM-A: Module in MSM-B is operational
03/17/2006 15:07:45.16 <Warn:DM.Warning> MSM-A: hal: ipmlSend of DM_MSG_CHKPT_DATA
failed with ipml_error -115 (errno 11)
```

(PD3-67727521)

Converging MVR with EAPS on a BlackDiamond 8800 Causes a Large Packet Loss

With MVR enabled on a BlackDiamond 8800, when the ingress port is on the egress-list this causes a high volume of traffic loss (PD3-62778911).

Intra-vMAN Traffic Does not Forward on an Ingress ACL

When configuring and applying a certain ingress ACL, traffic stops forwarding to ports belonging to the same vMAN. Removing the ingress ACL restores traffic (PD3-65450031).

Port-based Link Aggregation is not Currently Supported

vMAN link aggregation should support L2 aggregation by way of port-based and address-based link aggregation. Currently, only address-based aggregation is supported (PD3-65411141).

Configuring a Meter Value not Working Properly on a BlackDiamond 12804

When configuring a meter value using a large number, for example, 10,000 Gbps, on a BlackDiamond 12804 switch the CLI accepts the command. However, when you run the `show meter` command, an incorrect value is displayed (PD3-64743301).

Load Sharing is not Working with MAC-in-MAC

Packets are not transmitted on an enabled load sharing B-VLAN port from an S-VLAN port (PD3-62014321).

Deleting an S-VLAN from a B-VLAN Generates an Error

Deleting a service VLAN (S-VLAN) from a backbone VLAN (B-VLAN) generates the following error.

```
genesisResetVpifForNni: mismatch between realVlanId and nniVlanId
genesisResetVpifForNni: mismatch between realVlanId and nniVlanId
genesisResetVpifForNni: mismatch between realVlanId and nniVlanId
```

(PD3-58113221)

Extreme Networks Uses the Value 0x88B6 for the Ethernet Type for CFM

Extreme Networks is currently using the value 0x88B6 for the Ethernet type for CFM as the IEEE 802.1ag (PD3-58240961).

Disabling Load Sharing May Cause Temporary State Change

Enabling/disabling load sharing on ports while ESRP is running may cause temporary state changes (PD3-52741643).

Configuring an SSL Certificate Automatically Enables HTTPS

When an SSL certificate is configured, it automatically enables HTTPS. However, the `show ssl` command can show HTTPS as disabled (PD3-46782671).

disable mld snooping Command Should not Have Dependency on IPv4 Forwarding

The IPv6 CLI command `disable mld snooping` should not have any dependency on the state of IPv4 IP multicast forwarding (PD3-45280748).

MLD Query Reverses Maximum Response Time and Last Member Query Interval

The MLD v1 group specific query reverses the default value of Maximum Response Time and the Last Member Query Interval fields (PD3-45280304).

Switch May Stop Responding When Traffic Hits a Large ACL Policy

When creating a large policy file on a BlackDiamond 10808 switch and applying the policy to a VLAN on egress, if traffic is sent that attempts to hit the ACL rules, and the next hop ARP entry is not yet learned, the MSMs may stop responding (PD3-56415901, PD3-42385251).

MLD Snooping Entry Not Created if VLAN Does Not Have an IPv6 Address

On a BlackDiamond 8810 or Summit X450 switch, if a VLAN does not have an IPv6 address, the local MLD snooping entry is not created (PD3-48741446, PD3-37582541).

VLAN Statistic for rtif Interface is not Displayed

The VLAN statistic for the rtif interface is not displayed in ifTable/ifXTable (PD2-205017587, PD2-197340001).

802.1P Precedence Support

Incoming 802.1P precedence is not supported when ports are used for vMAN (PD3-24601141).

Disabling Smart Redundancy

After disabling smart redundancy on a port and then configuring the port and creating a VLAN, when you issue the `show vlan` command, the output displays *p1, *p2b. However, after you save the configuration and reboot the switch, the DUT may display *p1b, *p2 (PD3-46069035, PD3-35996092).

One Untagged port on Two VLANs with Different Protocols Can Cause Double Traffic

A port can be added in two VLANs as untagged ports if the VLANs are using different protocols such as "ip" and "any." When you send an IGMP Report, a membership is registered with the "ip" VLAN. By deleting the port from the "ip" VLAN, the membership gets removed instantly from "ip" VLAN, and upon a G.Q., membership is registered with the "any" VLAN now. Then, add the port back to "ip" VLAN, for 260 seconds, the port receives double traffic since membership are on both VLANs (PD3-40441999, PD3-19496831).

VLAN Mirroring Not Functioning Properly

VLAN mirroring does not work once you change the VLAN tag (PD2-223515075).

Clearing Neighbor Cache Can Cause Packet Drops

Clearing a neighbor cache with line rate traffic may cause delays in re-establishing the neighbor cache, which can result in packet drops. The delay can be avoided by temporarily pausing the line rate traffic, thereby allowing the neighbor cache to be re-established (PD3-29034388).

Different Algorithm for IPMC Traffic Egress on a Trunk

On a BlackDiamond 8810, due to a chipset limitation, IPMC traffic only egresses on one port of a trunk group, which is selected based on the order that the MSM sees link up conditions on the trunk group port. This is a different behavior than ExtremeXOS on a BlackDiamond 10808 (port-based or address-based), and the Summit E series (PD3-17186344).

OSPF

OSPF Process Not Starting After Running `restart process ospf` Command

It is not recommended that the OSPF process be restarted after a failover and before the backup MSM is fully synchronized (PD3-75244199).

OSPFv3

Changing Time While OSPFv3 is Learning Can Cause LSA to not Generate

If the system time is changed while OSPFv3 is running, LSAs may not generate and the routes may not be learned. To avoid this, run the `disable ospfv3` command followed by the `enable ospfv3` command to start OSPFv3 functioning properly (PD3-42948087).

Policy Manager

Incorrect Error Message When an Incorrect Policy is Configured Using BGP

The following incorrect error message is displayed when configuring a route policy using BGP:

```
* BD-10808.7 # config bgp neighbor 55.15.15.100 route-policy out nosales
BGP: Bind policy "nosales" failed!
No Error <<<<<<
Configuration failed on backup MSM, command execution aborted!
* BD-10808.8 #
```

(PD3-47374991)

Unsuccessful TFTP “Get” Removes the Existing File From the Switch

An unsuccessful TFTP Get or retrieval of a configuration file from the switch will remove the existing file from the switch (PD3-52371462).

QoS

Bandwidth Mode HQoS Traffic Cannot be Limited

When you configure three different services with the following HQoS parameters and send traffic with a peak rate for all services, 200M of traffic is sent out on an egress port instead of the expected 100M.

Service1 COS 2	20Mbps and can burst to maximum 100M if no other traffic is present.
Service2 COS 4	30Mbps and can burst to maximum 100M if no other traffic is present.
Service3 COS 5	50Mbps and can burst to maximum 100M if no other traffic is present.

(PD3-121372064)

Changing the Default Queue Profiles

The default queue profiles mapping remain intact even after deleting and adding the QoS profile on a Summit X450 or BlackDiamond 8800 switch (PD3-35119459, PD3-22513166).

Disabling Load Sharing or Deleting Member Ports from a Trunk

The member ports of a trunk will retain the QoS profile configuration of the trunk (based on the master port) after load sharing is disabled, or if a port is removed from the trunk (PD3-16578296).

RIPng

Cannot Bind Policy to RIPng Tunnel Interface

The following CLI commands cannot bind a policy to a RIPng tunnel interface:

- `configure ripng tunnel "abc" route-policy interface`
- `configure ripng tunnel "abc" trusted-gateway interface`

(PD3-54870635, PD3-44480254)

No Warning Message When Configuring More than 512 RIPng Interfaces

Configuring more than 512 RIPng interfaces on a BlackDiamond 10808 generates the following error message:

```
Configuration failed on backup MSM, command execution aborted!
```

On a BlackDiamond 8806 or Summit X450 switch, although only 512 RIPng interfaces are configured, there is no warning message that the command failed (PD3-54863764, PD3-41040185).

Malformed RIPng Packets

Malformed RIPng packets may be displayed in Ethereal (PD3-29034195).

RMON

Restart and Terminate do not Support snmpMaster and snmpSubagent

The restart and terminate process do not support the snmpMaster and snmpSubagent processes (PD3-46321054).

Trap Community String Octet Limits for Agent is Not Correct

trapDestCommunity allows octet string (0..127) but agent only support 32 characters strings (PD3-17622009, PD3-17622009).

clear counter Command Not Supported

Issuing the `clear counter` command might cause a high number to be displayed in variables such as etherHistoryOctets, etherHistoryPkts, and etherHistoryTable (PD3-12950492).

Alarm Entries Not Being Generated Correctly

Creating an alarm entry with an initial value of 0 for the alarm generates a falling alarm (PD3-17091355).

Routing Protocols

PIM Cache not Created when VRRP IP Address is used as Gateway

When VRRP is configured on a switch the PIM cache is not created when a VRRP IP address is used as a Gateway for static IP multicast routes (PD3-89812423).

Policies Configured on MVR Cannot be Refreshed

Do not refresh a policy configured on MVR.

Workaround. unconfigure and reconfigure the policy. For example,

```
configure mvr vlan v1 static group none
configure mvr vlan v1 static group <policy-name>
```

(PD3-63584999)

Security

Console Connection Allows Access to the Magic SysRq Facility

A console connection allows access to the Magic SysRq facility when using the Ctrl-V and Ctrl-X key combination at login (PD3-129475950).

User ACL Given Higher Preference over EAPS System ACL

When only one VLAN is created as a control VLAN for an EAPS domain, port and CPU utilization are high. This occurs only when a BlackDiamond 8810 is configured as an EAPS master and an access list is applied to the ring port (PD3-140962731).

Portions of the IP Security Feature set are not Supported with Static IP Addresses

The DHCP snooping, source IP lockdown, and DHCP secured ARP portions of the IP security feature set depend on DHCP assigned IP addresses and are therefore not supported with clients having static IP addresses (PD3-118747911).

Load Script Defaults TACACS Configuration to VR-Mgmt

Load script defaults the TACACS configuration to VR-Mgmt even when VR-Default is specified (PD3-124968250).

At Login, be Careful Entering Password after a Reboot

After a switch reboot and then entering a login user ID, wait for a "Password:" prompt before entering a password to ensure that the password is not visible (PD3-91606409).

RSA Key not Supported

When configuring SSH, use only the DSA public key. The RSA key is not supported in ExtremeXOS 11.6 (PD3-110736351).

Enabling IP Security on Link Aggregation Ports is not Supported

Enabling IP security features on link aggregation ports is not supported In ExtremeXOS 11.6. However, the CLI still allows configuring these features on link aggregation ports (PD3-109022651).

Authentication Using Dummy Primary and Secondary Servers Fails

Configure a dummy primary server and issue the `show session` and `show radius` commands. This should take approximately 14 seconds to execute. Running the same commands with a dummy secondary server takes approximately 15 seconds to execute. If you log out and log back into the switch it will take 15 seconds. During this time, multiple counters are incrementing in the `show radius` command output (PD3-102073084).

IP Security ACLs are not Shown for the `show access-list vlan` Command

If you use the `show access-list vlan` command, no IP security ACLs are shown (PD3-104389194).

DHCP Packets are not Relayed if `dhcp-snooping violation-action` is Set to None

When DHCP snooping is enabled on a port in a VLAN in monitoring only mode (that is, with the `violation-action` option set to `none`) and the switch is acting as a BOOTP relay, DHCP packets are not relayed from the DHCP server on that port. As a workaround, the port can be configured as a trusted-port (trusted for DHCP server packets) with DHCP snooping enabled with a `violation-action` of `drop-packet` instead of `none`. This works the same as setting the `violation-action` to `none` viz. The DHCP bindings database is built up by monitoring DHCP traffic but no rogue DHCP server traffic on that port is dropped (PD3-96212671).

RADIUS NAS-Port Attribute Should Display Without Slot Information

The RADIUS NAS-port attribute displays the port as 1024, instead of port 24 (PD3-77320136).

RADIUS NAS-Port Attribute is Missing for Network Login RADIUS Access Request Packets

The RADIUS NAS-port attribute is missing for Network Login RADIUS access request packets, but is included in the accounting packets (PD3-77320118).

`unconfigure radius` Command is not Clearing RADIUS Authentication and Accounting Counters

The `unconfigure radius` command does not clear the RADIUS authentication and accounting counters (PD3-75465301).

Unconfigure RADIUS and TACACS Does not Reset Timeout Value to System Default

The `unconfigure radius` and `unconfigure tacacs` commands do not reset the timeout value to the system default of 3 seconds (PD3-75120608).

RADIUS Authentication do not Work Correctly if Console Accesses the Backup MSM

If you are configuring a BlackDiamond 10808 or BlackDiamond 8810 with RADIUS authentication, when telnet or console access is through the master MSM, RADIUS authentication works correctly. However, if console access is through the backup MSM, RADIUS authentication does not work correctly and generates the following error message:

```
<Erro:AAA.RADIUS.serverNotInit> MSM-B: Authentication server for Switch Management is not initialized
```

(PD3-74708933)

icmpInMsgs Counter Displays only Incoming ICMP Packets

icmpInMsgs counter will display the incoming ICMP packets for VR-Default only (PD3-39411271).

extremePortLoadshare MIB Table Empty When Load Sharing is Enabled

Enable load sharing on a port and run the `show ports configuration` command. Even though the command output shows that load sharing is enabled on the port, the extremePortLoadshare table is empty (PD2-204685753, PD2-196089286).

Changing a Password after Password Expiration Terminates SSH Session

When a local user password expires, logging into the switch using SSH will prompt you to change your password. After changing the password, the current SSH session will be terminated and you will need to login to the switch using the new password (PD3-29911678, PD3-29948301).

ETHER-P-8021Q is Not a Valid Match Criteria

ETHER-P-8021Q is not a valid ethernet-type match criteria and generates a syntax error. You can use 0x8100 (PD3-29818741).

Upgrading and Rebooting a Backup MSM

If the configuration files on both MSMs are the same and the following warning message is displayed, you can safely ignore the message.

```
11/23/2004 07:46:16.21 <Warn:cm.configNotInSync> Backup MSM has different configuration files than primary MSM. Auto configuration file synchronization will be performed.
```

(PD3-20833318, PD3-18042351)

sFlow

sFlow Will Accept Invalid IP Addresses for Collector Address

sFlow will allow you to configure invalid IP addresses as sFlow collectors. Only valid unicast IP addresses should be used to configure the sFlow collector (PD3-40462478, PD3-27536575).

sFlow May Not Sample Correctly with Heavy Traffic

sFlow may not sample frames at the correct rate on BlackDiamond 8800 switches during periods of heavy ingress traffic on the specified port (PD3-19287440, PD3-19377255).

SNMP

SNMP MIB Query not Returning Consistent Value for Egress Port Bandwidth Use

An SNMP MIB query does not return a consistent value for egress port bandwidth utilization (PD3-131944211).

Modifying IP Addresses through SNMP is not Possible

You cannot configure a netmask alone when configuring an extremeVlanIpEntry on a VLAN. Users have to set both IP address and netmask on a VLAN. If you want to configure netmask on a configured VLAN with an IP address, unconfigure the current IP address and set both the fields at once (PD3-96576791).

Smart Traps not Generated while Adding a Trap Rule IP Address

Smart traps are not generated if the smart trap rule ipAddrTable is configured (PD3-47804527).

Some Objects in icmpGroup May Return Incorrect Values

When initiating an outgoing ping from the switch, the following counters do not increment.

- icmpOutMsgs
- icmpOutEchoReps

(PD3-42395376)

alarmTable Does Not Validate the alarmVariable

Creating an alarmTable entry does not validate the alarmVariable and does not generate a badValue error message (PD3-12761053).

Spanning Tree Protocol

CLI Does not Show a Clear Error Message when Configuring STP

When the same port is added in dot1d mode to two different STP domains, ExtremeXOS switches are not providing a clear error message (PD3-123227322).

When a Port Becomes an Alternate Port, the Switch does not send out an Alternate Proposal

When a port becomes an alternate port, the switch does not send out an alternate proposal for that port. Therefore, the designated port goes through 30 seconds of listen and learning (PD3-92702567, PD3-105062392).

CIST Ports Remain in Disabled State

CIST ports remain in the disabled state when MSTP is configured in a specific order (PD3-75882801).

Backup MSM Crashes When Disabling STP with MSTI and CIST Enabled

When MSTI and CIST are enabled, executing the `disable stp` command causes the backup MSM to crash (PD3-76712731, PD3-65171107).

Removing MSTI Root or Making MSTI Root Inferior can Cause Topology Changes

With multiple alternate ports, removing MSTI root or making MSTI root inferior can cause several topology changes. MSTI can take up to 30 seconds to converge (PD3-67562861).

Sending or Receiving Inferior BPDUs

Some traffic will be dropped when receiving inferior BPDUs (PD3-17340398, PD3-13016876).

SSH

ssh.xmod Must be Installed to Configure SSL Certificates

ssh.xmod must be installed to configure SSL certificates. If ssh.xmod is not installed on the switch, configured SSL certificates are not loaded into the switch and no error is returned (PD3-29939091).

Uninstalling SSH Image Causes Watchdog Reboot

Uninstalling an SSH image causes the watchdog to reboot. After the switch restarts, only one MSM SSH image is uninstalled before the watchdog reboot starts.

Workaround. Wait 5 seconds before uninstalling SSH.

(PD3-35827551)

MSM-B Does Not Accept SSH Connection

A BlackDiamond 8810 MSM-B may not accept SSH connections after an MSM failover is triggered. The output of the `show management` and `show process` commands will still display the correct SSH2 information.

Workaround. Terminate the `exsshd` process using the `terminate exsshd process graceful` command then restart the process using the `start process exsshd` command.

(PD3-20746381, PD3-20121506)

Regenerating an SSH Key

After regenerating the SSH key you must save the configuration and then terminate `ssh`. Terminate the SSH process using the `terminate process exsshd graceful` command and then restart the process using the `start process exsshd` command (PD3-14620801).

Verify SSH Module and SSH Image are the Same

When downloading an SSH module, ensure the module is the same as the image. For example, 11.1.0 image will only allow 11.1.0-ssh module (PD3-11563811).

SSH2

DES Cipher Fails Authentication

Attempting to login to the switch with a "des" cipher fails authentication and generates the following message:

```
warning: Authentication failed.
Disconnected; key exchange or algorithm negotiation failed.
```

(PD3-60673957, PD3-39739546, PD3-26746401)

System Related

Static Route Forwarding Does Not Forward to a Second Link

In a multiple switch configuration, if two switches have two links and share static route forwarding, if the first link forwarding traffic has `ipforwarding` disabled, the traffic does not resume with the second link that still has `ipforwarding` enabled (PD2-241021669, PD2-222627405, PD2-210437928).

Disabling IP Forwarding on a VLAN

When disabling IP forwarding on a VLAN associated with the first static route, IP forwarding is stopped (PD3-35694597).

show log Error Messages

Messages stored in NVRAM are in encoded format. To restore the ASCII text of a message, the version of ExtremeXOS loaded must be able to interpret the data written prior to reboot. When the encoded format for a particular message cannot be interpreted by the version of ExtremeXOS currently loaded, the messages are displayed in the following format.

```
03/21/2005 17:15:37.36 <UNKNW:epm.28> : NO MESSAGE DECODE; Missing component "epm"
v24.2
                                DUMP-00: 00 2C 00 01 FF FF FF FF 00 00 00 95
42 3F 71 B9 '.,.....B?q.'
                                DUMP-10: 00 14 C3 C1 00 11 00 1C 01 FF 00 08
65 70 6D 00 '.....epm.'
                                DUMP-20: 08 FF 00 0C 00 18 00 02 65 70 6D 00
'.....epm.'
```

(PD3-28577971)

Unknown Card Type Error Message

The following message is displayed on the console when a module is present that the current image does not support:

```
Error: Unknown card type in slot X, please remove!
```

ExtremeXOS will not check-point sync the switch until the incorrect module is removed (PD3-28631368).

UPM

LLDP is Showing Power in Tenths of a Watt

The variable EVENT.DEVICE_POWER now displays power in milliwatts when an LLDP device is detected. For example, 5.7 watts it now shown as 5700 (PD3-124182761).

VLAN

SVLAN and BVLAN Cannot Share the Same Physical Port

An SVLAN and a BVLAN cannot share the same physical port (PD3-65267086).

VRRP

VRRP is not supported on User-Created VRs

VRRP is not supported on user-created VRs in ExtremeXOS 11.6.2 (PD3-95689131).

MSM Failover on VRRP Backup Node Causes VRRP State Change

An MSM failover causes a VRRP state change when running 128 virtual routers in the backup state on a BlackDiamond 8800 and a BlackDiamond 12804 (PD3-54695903).

Configuring Advertised Intervals at 100 ms May Cause Dual Masters

Configuring an advertised interval at 100 milliseconds with more than 64 VRRP instances may cause dual masters on the BlackDiamond 8800 series, BlackDiamond 10808, and BlackDiamond 12804 switches (PD3-95938607).

Data Packets will not be Forwarded When Configuring VRRP with vrid ≥ 7

On a BlackDiamond 10808, if you configure VRRP with seven unique VRIDs, and configure one or more ESRP domains, data packets will not be forwarded on one of the eight virtual MACs. Therefore, when the last domain is enabled, it will not be allocated a virtual MAC and will not forward traffic. The domain that will not forward traffic will be the last domain that is enabled, which can vary. To avoid this situation, do not configure ESRP and VRRP at the same time (PD3-54852211, PD3-41952782).

High CPU Load Causes VRRP Flipping

Creating heavy CPU loads on a BlackDiamond 8810 switch may cause VRRP to enter a dual master state. For example, a large EAPS configuration failing over puts a heavy load on the CPU (PD3-23903481, PD3-17993197).

XENPAK SR

When Changing Gigabit Links, the Link Light Being Up Does Not Guarantee Traffic Flow

When changing from a 1 gigabit link to a 10 gigabit link, the link light does not guarantee that traffic is flowing. If traffic is not flowing properly even when the link light is up, this may be an issue with the cable or XENPAK. If you experience a problem, it is advisable that a LX4 XENPAK be used since it can also be used with a multimode cable and is capable of transmitting over a longer distance (PD3-74839191).

Documentation

“configure vpls” Command Default for dot1q is Incorrect

The default for the keyword `dot1q` used in the `configure vpls` command should be `exclude not include` as stated in the *ExtremeXOS 11.6 Command Reference Guide, Software Release 11.6* (PD3-114942811).

“configure ospf import-policy” Command Does not Filter Routes

The `configure ospf import-policy` command does not filter routes from being added to routing tables as stated in the *ExtremeXOS 11.6 Command Reference Guide, Software Release 11.6* (PD3-90901731).

“show inline-power info detail” Command Output Differs from Documentation

On the Summit X450a, the `show inline-power info detail` command output is different from that shown in the documentation. For this platform only, the `priority` field is not displayed. Priority only applies to the modular PoE devices (PD3-78599376).

“show inline-power” Command Output Differs from Documentation

On the Summit X450a, the `show inline-power` command output is different from that shown in the documentation. For this platform only, the `disconnect precedence` and `budgeted power` fields are not displayed. These only apply to the modular PoE devices (PD3-78599401).

Issues Resolved in ExtremeXOS 11.6.3.5

The following issues were resolved in ExtremeXOS 11.6.3.5. Numbers in parentheses are for internal use and can be ignored. ExtremeXOS 11.6 includes all fixes up to and including ExtremeXOS 11.1.4.4, ExtremeXOS 11.2.3.3, ExtremeXOS 11.3.4.5, ExtremeXOS 11.4.4.7, and ExtremeXOS 11.5.2.10. For information about those fixes, see the release notes for the specific release.

BlackDiamond 8800 Series of Switches

Running diagnostics no longer fails on certain I/O modules on the BlackDiamond 8800 series of switches (PD3-173055969).

Issues Resolved in ExtremeXOS 11.6.3.4

The following issues were resolved in ExtremeXOS 11.6.3.4. Numbers in parentheses are for internal use and can be ignored. ExtremeXOS 11.6 includes all fixes up to and including ExtremeXOS 11.1.4.4, ExtremeXOS 11.2.3.3, ExtremeXOS 11.3.4.5, ExtremeXOS 11.4.4.7, and ExtremeXOS 11.5.2.10. For information about those fixes, see the release notes for the specific release.

BlackDiamond 8800 Series of Switches

I/O modules no longer crash when a management port goes into an inactive state from an active state in ExtremeXOS 11.6.3.3 (PD3-170096006).

Issues Resolved in ExtremeXOS 11.6.3.3

The following issues were resolved in ExtremeXOS 11.6.3.3. Numbers in parentheses are for internal use and can be ignored. ExtremeXOS 11.6 includes all fixes up to and including ExtremeXOS 11.1.4.4, ExtremeXOS 11.2.3.3, ExtremeXOS 11.3.4.5, ExtremeXOS 11.4.4.7, and ExtremeXOS 11.5.2.10. For information about those fixes, see the release notes for the specific release.

General

ExtremeXOS software log filters now support multiple filter instances on the same event and parameters (PD3-91684711).

An MSM with a higher node value now has a higher priority over an MSM with a lower node value (PD3-121647603).

ExtremeXOS suppresses log messages for spurious AC PSU input voltage readings. A single spurious value reported by an AC PSU is ignored by ExtremeXOS rather than logged as an increase in voltage, immediately followed by a decrease in voltage. This occurs on BlackDiamond 8800, BlackDiamond 10808, and BlackDiamond 12804 switches (PD3-133686361, PD3-133203289).

An assertion error no longer occurs when a 10G link between a BlackDiamond 12800 series switch flaps while streaming multicast traffic through an EAPS ring (PD3-153103211, PD3-149584659).

A switch configured with console logging enabled no longer experiences unexpected reboots as a result of an EMS server being killed by EPM (PD3-149530611).

Consecutively uploading an image to a switch using SFTP followed by entering the `install image` command, without terminating the original SSH session, no longer causes the switch to reboot during the installation (PD3-140703992, PD3-141735501, PD3-153125358).

A switch no longer reboots due to a timer wraparound after 497 days of uptime (PD3-132912714).

BlackDiamond 8800 Series of Switches

The Ethernet link between a BlackDiamond 8810 and other networking equipment no longer comes up regardless of the cable type (crossover or straight through) connected to the port even when the autopolarity feature is disabled (PD3-125226932).

Stack monitoring no longer causes BlackDiamond 8810 I/O modules to fail when processing large ACL lists and cascaded interrupts (PD3-135010821).

When multicast streams are egressing on a BlackDiamond 8800 switch using a 10G4X port for multiple VLANs, adding a multicast cache entry for a new stream egressing through the same port no longer results in packet loss for the existing multicast streams. In addition, deleting a multicast cache entry

egressing through the same BlackDiamond 8800 10G4X port no longer results in packet loss of other multicast streams (PD3-139911651).

When multiple multicast streams are egressing on the 10G4X port of a BlackDiamond 8800 switch for multiple VLANs, deleting the multicast cache for one of the multicast streams no longer prevents the stream from egressing the port (PD3-138646273).

BlackDiamond 10808 Switch

When cold rebooting a BlackDiamond 10808, an MSM with a higher node priority always becomes the master. In case of equal node priority, MSM-A becomes the master (PD3-92509787).

An MSM failover caused by a deadlock in the CPU packet driver is no longer seen (PD3-136756301, PD3-136615381).

BlackDiamond 12800 Series Switches

Packets with IP options are no longer egressing BlackDiamond 10808 switches with an incorrect IP header checksum (PD3-92903593).

The `show configuration` command output is now displayed correctly when creating a virtual router and associating it with a VLAN (PD3-124953726).

On a BlackDiamond 12800 series switch, the Policy Manager no longer crashes when an ACL policy is refreshed (PD3-122689936).

A HAL process crash is no longer encountered when a multicast destination address is added to a policy and the policy is refreshed (PD3-125543791).

The output for the `show platform ipv4mc` command now displays the correct number of IGMP groups (PD3-145465011).

Summit Family of Switches

A Summit X450a or X450e series switch no longer experiences voice jitter in half duplex mode when simultaneously running an FTP data transfer session (PD3-137927261).

The MAC limit-learning feature has been enhanced with a `stop-learning` argument that protects the switch CPU from exhausting FDB resources with blackhole entries.

```
configure port <portlist> vlan <name> [limit-learning <number> {action [blackhole | stop-learning]} | lock-learning | unlimited-learning | unlock-learning]
```

When limit-learning is configured with `stop-learning`, the switch CPU is protected from exhausting FDB resources by not creating blackhole entries. Any additional learning and forwarding is prevented, while not impacting packet forwarding for existing FDB entries.

On Summit X450 series switches, when the configured learn limit is reached on a single VLAN, additional learning and forwarding on a port is stopped, which impacts all the VLANs configured on that port. All other platforms (BlackDiamond 10808 switch, BlackDiamond 12800 series switches, BlackDiamond 8800 series of switches, Summit X450a and X450e switches) only the VLANs in a port are impacted when the configured learn limit is reached (PD3-83420814).

Traffic forwarding continues in a LAG and software controlled redundant port environment after the primary port has been disconnected and reconnected (PD3-129851001).

Combo ports on a Summit X450 switch with SX or dual speed SFP 100/1000 FX/LX GBICs are no longer in the Ready state after a switch reboot with auto off (PD3-125519998).

Configuring an ACL with a syntax error in the policy file no longer causes a Summit X450 switch to reboot (PD3-121846211).

ACL

Applying a VLAN translation ACL now works properly and traffic is no longer forwarded with the same inner tag (PD3-120701781).

If you apply an ACL that implements Policy Based Routing in a mixed module environment, the ACL will be rejected if it applies to any original series modules. The error message displayed is the same with or without a backup MSM-G8X (PD3-149418543).

A refresh policy now releases ACL mask entries (PD3-139548904).

Using the policy file `uplinkport.pol` no longer causes packets to be dropped in the switch (PD3-100723201, PD3-100178561).

BGP

A BGP neighbor IP address check is no longer performed per classful network (PD3-120895991).

CLI

A typographical error has been corrected in the `show configuration nettools` command output (PD3-103768641).

The `show fdb` command now contains the parameter `blackhole {netlogin [all | mac-based-vlans]}`, which specifies blackhole entries (PD3-98232360).

The command output for the `show sflow <tab>` command has been corrected for typographical errors (PD3-98288559).

The `show ipstats` command now increments IGMPv3 statistics (PD3-94304801).

Control Protocols

Address-based load sharing ports no longer stop forwarding multicast traffic if a link is disconnected (PD3-120092845).

Device Management

The `show power` command output no longer shows the input voltage value for the Summit X450 series switch (PD3-126551866).

ExtremeXOS now allows a port display string length to be a maximum of 20 characters (PD3-137828410).

Configuring WAN PHY ports on a primary MSM using an LW XENPAK no longer displays error messages on the backup MSM (PD3-154844322).

Error messages now contain more definitive information when upgrading an ExtremeXOS image containing a VLAN name (PD3-122558012).

SNMP trap packets are sent out with the source IP address configured in the `configure snmp add trapreceiver` command (PD3-128206723).

In ExtremeXOS 11.6, the SNMP table command is can now query the entPhysicalTable of the Entity MIB (PD3-91687841).

extremeRmonEnable no longer returns a value of zero in ExtremeXOS devices even after enabling RMON using the CLI, it now returns a value of true (one) (PD3-88020132).

The `config ipmcforwarding to-cpu off ports <port-list>` command is now applied to all ports specified in the port-list after a save and reboot (PD3-142477386).

When a backup MSM is in SYNC, all routes are now updated across redundant systems (PD3-129285523).

Port utilization is now reported correctly on 10G ports (PD3-120945271).

Documentation

EAPS

Whenever an ingress port for multicast traffic changes, earlier IGMP snooping cache entries are deleted and re-created with the new ingress port (PD3-135281102, PD3-136669244).

Adding a secondary port to an EAPS protected VLAN while the secondary port is down or disabled no longer causes a loop when the secondary port comes back up (PD3-133764885).

ESRP

When using ESRP extended mode and a default election algorithm with load sharing in ExtremeXOS 11.5.2.10, when one of the LAG member ports is disconnected on the master load-shared port, the ESRP state changes to slave. This does not occur in ExtremeXOS 11.6.2.9 even though the master load-shared port weight is adjusted (PD3-137374198).

IP multicast packets ingressing on load shared ESRP host attach ports are now forwarded out on other ports (PD3-111598147).

VLAN ports are now in the blocked state when a BlackDiamond 8810 becomes an ESRP slave after an MSM failover (PD3-131891883).

IP Routing Protocols

RPF path selection for multicast over ECMP now gives a high preference to a routing entry with a high IP address nexthop. This new RPF selection reduces the possibility of PIM assert occurrences in a real environment because PIM assert gives a higher preference to the higher IP address if the metric S,G state information is the same (PD3-126861436).

An ARP adjacency for a next-hop IP address is no longer lost when a switch experiences a scanning attack, causing numerous incomplete ARP entries (PD3-137634792, PD3-137467561).

VLAN names that include the `mgmt` prefix now appear in the `show igmp snooping` command output (PD3-141235103).

A BGP routing policy that contains an entry with a deny action and any one of the other actions such as "community, as-path, or nlri," no longer causes the BGP process to crash (PD3-137209972).

A route manager task crash no longer occurs within three minutes of disconnecting and reconnecting an iBGP neighbor. The task crash occurs earlier and only when the switch is configured to export a default route into BGP (PD3-124609842).

ARP entries are now learned during peak traffic and an MSM failover (PD3-129285787).

Route replacement by the route manager no longer results in duplicate/stale BGP routes in the IP routing table (PD3-133764554, PD3-114042562).

IPv4 Multicast

Multicast cache entries are now updated in hardware after an MSM failover (PD3-156370064).

BlackDiamond 10808 switches no longer experience a HAL process crash when L3 IP multicast entries are removed from hardware (PD3-152387720).

After running multiple MSM failovers, IPv4 multicast entries entry no longer shows 15,128 streams rather than 10,000 streams (PD3-153103182).

Egress port information in the hardware IPv4 multicast cache entry is no longer out of sync with the software IPv4 multicast cache entry (PD3-125375605).

MPLS

When disabling MPLS with a large number of VPLSs, the VC labels associated with a VPLS session are no longer removed, which was resulting in the wrong labels being programmed into the hardware (PD3-130951077, PD3-99484115).

When numerous RSVP-TE LSPs are configured, enabling and quickly disabling RSVP-TE no longer causes data corruption, resulting in a system crash (PD3-130968992, PD3-125485371).

When an OSPF database exchange occurs, if the LSID for the OSPF router address has changed and the neighbor's version must be flushed, for example, after a reboot, the router address is no longer purged from the CSPF database (PD3-104046299).

Changing the Ethernet type on a VPLS service vMAN no longer causes the device to stop forwarding traffic (PD3-130672063, PD3-128184768).

Network Tools

Continuously disabling and enabling MPLS using the `disable mpls` and `enable mpls` commands no longer leads to a memory resource shortage (PD3-137613771, PD3-128400391).

Console and telnet sessions no longer hang when processing an SNMP get request for a transmission group (PD3-146439617).

Log timestamps in the `show log` command output now match the time displayed in the `show switch` command output (PD3-121149464).

The `configure snmp broadcast` command now includes the argument `vr <vr_name>` to correctly respond to SNMP broadcast traffic (PD3-108984534).

ExtremeXOS shell sessions (exsh) invoked by a telnet session are now terminated after a session is closed (PD3-152513845, PD3-152169000).

The netTools process no longer experiences an increase in memory usage when a DNS server returns a lookup failure for a hostname (PD3-146565529).

Network Services

A route manager process crash no longer occurs when configuring 6to4 tunnel and IPv6 static routes. This crash was observed when the overlapping IPv6 subnet was configured on a 6to4 tunnel and IPv6 interface (PD3-86441744).

The CLI now shows error messages when a mask for an Ethernet destination address is given in a policy file without using the `mask` keyword (PD3-123322724).

The ExtremeXOS CLI now allows users to omit the leading zero of a MAC address (PD3-106860138).

Traffic is no longer dropped by the ACL meter with committed-rate or max-burst-size configurations (PD3-108733401).

MSM failover traffic is now egressing ports with QoS configured (PD3-153078418).

In a dual MSM configuration, when FDB entries are flushed on the primary MSM, the backup MSM correctly flushes the same entries to remain in sync with the FDB table on the primary MSM (PD3-150090401, PD3-126162701).

When a port that is disabled for a jumbo frame is added to a vMAN using ExtremeXOS, jumbo frames are now forwarded by the switch (PD3-102568888, PD3-102568858).

OSPF

ExtremeXOS software uses a new flag "f" to signify routes that are provided to the FIB. When ECMP is not enabled, only the active route that is installed in the hardware will contain the "f" flag.

```
* (debug) BD-12804.39 # show iproute
Ori Destination      Gateway      Mtr  Flags      VLAN      Duration
#s  Default Route    110.110.116.2  1    UG---S-umf-- vlan107    0d:0h:5m:50s
#s  Default Route    110.110.117.2  1    UG---S-um--- vlan108    0d:0h:5m:50s
#s  Default Route    110.110.118.2  1    UG---S-um--- vlan109    0d:0h:5m:50s
```

Flags: (B) BlackHole, (D) Dynamic, (G) Gateway, (H) Host Route
 (L) Matching LDP LSP, (l) Calculated LDP LSP, (m) Multicast
 (P) LPM-routing, (R) Modified, (S) Static, (s) Static LSP
 (T) Matching RSVP-TE LSP, (t) Calculated RSVP-TE LSP, (u) Unicast, (U) Up
 (f) Provided to FIB

(PD3-122520931)

QoS

When streaming IPv6 traffic across a BlackDiamond 10808 routed IPv6 VLAN with dot1p values, the output for the `show port qosmonitor` command no longer shows the wrong egress port (PD3-121836520, PD3-77710211).

Security

DHCP snooping and ARP entries are now removed when a Summit X450 series switch receives a DHCP release packet (PD3-135845805, PD3-135530701).

Configuring a RADIUS server with a host name no longer causes a switch to stop responding, or in some cases hang (PD3-106859881).

sFlow

Inbound packets are no longer dropped when sFlow is enabled on a Summit X450a switch (PD3-123323041).

sFlow samples are no longer forwarded to the egress port, which was resulting in duplicate packets (PD3-134495516).

SNMP

Polling the `extremeVlanIfStatus` (object OID `.1.3.6.1.4.1.1916.1.2.1.2.1.6`) no longer returns a result of active for a VLAN interface. The result is “not ready” or “not in service” (PD3-118437141).

Walk Extreme-FDB-MIB object now returns values the same as the Summit 400-48t (PD3-116975701).

Spanning Tree Protocol

Reflecting STP BPDU with agreement is correctly processed for fast convergence for RSTP point-to-point connections (PD3-128034776).

STP topology changes no longer cause an FDB flush on all ports of a specific VLAN ports, including the non-assigned STPD VLAN ports (PD3-137936946, PD3-137501673).

SSH2

CLI commands allowed by a user profile are no longer erroneously rejected after the user accesses the switch using SSH (PD3-145933614).

Stacking

VRRP VLANs are no longer lost after an MSM failover, which was causing L3 traffic to be dropped (PD3-152921600).

vMAN

When the last vMAN is removed from a port configuration, multicast traffic continues to be forwarded to the CPU (PD3-131181001).

Changing the vMAN EtherType to 0x8100 now forwards traffic on the correct link of a load-shared group based on the load sharing algorithm. However, vMAN does not support L3_L2_CHK_SUM and L2_L3_L4 algorithms. For a DSCP QoS issue, apply an explicit vMAN ACL (PD3-124163388).

Issues Resolved in ExtremeXOS 11.6.2.9

The following issues were resolved in ExtremeXOS 11.6.2.9. Numbers in parentheses are for internal use and can be ignored. ExtremeXOS 11.6 includes all fixes up to and including ExtremeXOS 11.1.4.4, ExtremeXOS 11.2.3.3, ExtremeXOS 11.3.4.5, ExtremeXOS 11.4.4.7, and ExtremeXOS 11.5.2.10. For information on those fixes, see the release notes for the specific release.

General

Software enhancements to comply with the new Daylight Saving Time (DST) changes applicable for year 2007 are now complete (PD3-122115813).

While upgrading a software image to ExtremeXOS 11.6, you no longer need to download and install the image on both MSMs (PD3-107465701).

BlackDiamond 8800 Series of Switches

Disabling a slot using the `disable slot <slot>` command now turns off I/O module LEDs as stated in the *ExtremeXOS Command Reference Guide* (PD3-76068785).

Conduit errors no longer lead to a slot failed state when running simple traffic tests (PD3-103199501, PD3-78210348).

IPv4 adjacency log messages with "Table full" are no longer erroneously logged by BlackDiamond 8800 series I/O modules (PD3-99627491, PD3-98893708).

You can now upgrade a BlackDiamond 8800 series switch using the hitless upgrade procedure shown in [“Upgrading the Active Partition Using Hitless Upgrade” on page 29](#) (PD3-108778071).

ARP replies and L3 misses now get to the CPU when they are received on a load sharing member port other than the configuration master port (PD3-110126951).

The node priority on an MSM B can now be set to a default value of zero (PD3-86434438).

IPv4 multicast Table Full error log messages are no longer erroneously generated on Black Diamond 8810 switches using G48Ta, G48Te, and G48Pe I/O modules (PD3-118697351).

BlackDiamond 10808 Switch

Slow memory depletion in the FDB process has been corrected (PD3-92094777).

When configuring mirroring on a BlackDiamond 10808, mirroring behavior no longer changes for L2 packets in a VLAN if the VLAN tag is changed (PD3-118320690, PD3-63541181).

An MSM (initial master) no longer reboots every 12 minutes after an initial two to three hours into a virtual router flap test (PD3-92528887).

Removing an Avaya VoIP phone from an LLDP enabled port no longer generates an error message in the log (PD3-85075931).

Issuing the `save configuration` command on a BlackDiamond 10808 running G60X modules no longer causes the switch to crash and display an error message (PD3-73842161).

BlackDiamond 12800 Series Switches

MAC addresses are no longer aging out at 300 and are now reset to 0 (PD3-119446388).

Forwarding no longer stops for ECMP routes after an MSM failover (PD3-104348785, PD3-85351151).

The system clock on a BlackDiamond 12804 switch no longer loses an average of 10 seconds per day (PD3-83939958, PD3-75525627).

Summit Family of Switches

An insufficient power message is no longer displayed when performing a cold boot on a Summit X450 series switch (PD3-92509429).

The Summit X450 switch now supports the L3 load sharing algorithm (PD3-98545221).

Slow path transmission of IP control protocols is no longer impacted by low priority traffic congestion on the data path (PD3-119104958).

A stack overflow no longer causes a Summit X450 switch to reboot in some cases (PD3-111000131, PD3-112515433).

ACL

When configuring a system counters policy file for a port or VLAN, the system counters are now being sampled (PD3-57827749).

Egress ACL counters for slow-path forwarded IP packets are no longer counting twice the actual packets (PD3-94304671, PD3-100210971).

Unconfiguring or refreshing an ACL policy containing approximately 1,400 rules no longer causes a hardware failure (PD3-107306981, PD3-104370195).

Applying an ACL policy file to a BlackDiamond 8810 running ExtremeXOS 11.5.2.10 using the `configure access-list any ingress` command no longer fails due to a stack size overflow crash (PD3-111229133).

CLI

CLI commands related to TFTP no longer stop working after long periods of time using a TFTP server that does not support the block size option (PD3-97327209).

ExtremeXOS 11.6.2.9 now includes a `clear session history` command (PD3-77995201).

Control Protocols

Disabling ELSM on a load sharing port and then enabling ELSM on the same port no longer stops multicast switching (PD3-103567967).

ELSM

ELSM packets egressing a BlackDiamond 10808 or BlackDiamond 12804 switch are no longer too short, which was causing them to miss the frame check sequence (PD3-112938164, PD3-112636560).

ESRP

When ESRP port mode is set to host, the ESRP master can now ping the host connected to the slave host port (PD3-90047432).

IP Routing Protocols

A new CLI command, `enable/disable igmp proxy-query vlan <vlanname>`, has been introduced to enable and disable sending IGMP proxy queries with an L2 VLAN (PD3-155226621).

A PIM task crash is no longer seen in a PIM BSR environment in a triangle topology (PD3-122496001).

If the next hop for a route is a link local address and that same link local address is also associated with another adjacency, but with a different VLAN ID, the next hop is properly installed in the hardware tables and IPv6 traffic destined for that route is forwarded in the slow path (PD3-98820711, PD3-97208236).

After changing a VLAN tag, multicast switching using MVR ingress through the VLAN no longer stops on Summit X450 platforms (PD3-100013857).

IPv6 Unicast

When running the `show neighbor-discovery ipv6 cache` command, the link local IPv6 address entry from other ExtremeXOS switches is no longer high, causing the entry to not age out (PD3-41595507).

The IPv6 neighbor cache is learned after making gateway interface changes from a normal IPv6 VLAN to a tunnel (PD3-32690078).

MPLS

When configuring a BlackDiamond 10808 with two Ethernet connections and each connection has an ERO pointing to the Ethernet side of the connection, the label switching path now connects properly with the EROs (PD3-67444691).

Errors are no longer seen when issuing a `disable port` command followed by an `enable port` command for the transmit port of the primary path of an RSVP-TE LSP (PD3-85712828).

The `show mpls rsvp-te bandwidth` command no longer displays an error when a VLAN is specified (PD3-92598971)

When a switch is configured for 100 VPLS pseudo wires and you issue the `run msm-failover` command, an error is no longer displayed (PD3-100785071)

Some MPLS ECMP topologies no longer have old label switched path (LSP) data programmed on the backup MSM after a failover event from the primary MSM to the backup MSM (PD3-107645786).

IGMP control messages are now flooded across VPLS (PD3-108934009).

Network Login

Web-based Network Login now accepts passwords containing a “%” character (PD3-112891158).

Using web-based network login, a device now responds with a DHCP NACK to a DHCP REQUEST after authentication (PD3-96601395).

Using web-based Network Login, the RADIUS VSA Extreme-Netlogin-Url-Desc cannot be more than 80 characters (PD3-39395847).

Network Login dot1x authentication now supports Microsoft's Network Access Protection (NAP) Remediation server (PD3-106669537).

Configuring a web-based Network Login base URL with more than two sub-domains, such as “netlogin-testing.rtp.extremenetworks.com” no longer fails (PD3-64359611).

Network Services

ICMPv6 packets can now be blocked using the ethernet-type 0x86dd field in the ACL (PD3-50933163).

Packet performance has been improved when sending packets to the CPU during a moderately high traffic rate of broadcast packets. Ping and telnet response time has also improved (PD3-116108048).

Disabling and enabling a port in slot 1 with STP enabled no longer shows an FDB error in the log (PD3-92471344)

Security

When a UDP profile is configured to forward traffic to a VLAN on a switch, traffic is now sent out with the destination MAC address set to broadcast MAC (PD3-96530041).

Clients logging into a switch using MAC-based Network Login are no longer shown as unauthenticated after an MSM failover (PD3-93609317).

When the switch boots, saved policy files are synchronized to slots using the correct precedence. This applies to BlackDiamond 8800 original series modules (MSM-G8X modules, and G24X, G48T, G48P, and 10G4X I/O modules)(PD3-103693995, PD3-102421416).

You no longer have to make sure you unconfigure all the ACLs applied to a VLAN before changing the VLAN tag (PD3-107346365, PD3-24794592, PD3-57946832, PD3-26612201).

Using telnet and ping from a client PC directly connected to a DUT interface now works correctly when DHCP snooping is enabled (PD3-98168656).

When two DHCP servers are configured on a switch, the command output for the `show ip-security dhcp-snooping violations vlan def` command is now showing multiple violation entries (PD3-108689851).

When IP security is configured in a BOOTP relay scenario, a DHCP release packet from the DHCP client now removes the corresponding entries from the DHCP snooping table (PD3-107650230).

The password can now be changed after logging in to a switch with a user account (PD3-119521493).

Spanning Tree Protocol

After configuring STP Operational mode dot1w, added ports no longer show the old default port priority range (16) (PD3-1029362720).

SSH2

Users no longer need to specify /scratch directory to upload an image (.xos or .xmod) to the switch (PD3-111696727).

Using SFTP, "ls" no longer closes the connection (PD3-111041575).

Universal Port Management

Users can now see variables when running a profile on a RADIUS server using VSA (PD3-121860301).

Accidentally configuring a port twice on an event no longer triggers the UPM profile twice. You can delete the profile and create the UPM profile followed by the event (PD3-109022611).

vMAN

A CLI feature is provided to disable multicast processing on a port on Summit X450 and BlackDiamond 8800 switches. When this feature is enabled, an IP multicast cache is no longer created when a port belongs to multiple vMANs and one of the vMANs is configured with an IP address (PD3-118752917).

Issues Resolved in ExtremeXOS 11.6.1.9

The following issues were resolved in ExtremeXOS 11.6.1.9. Numbers in parentheses are for internal use and can be ignored. ExtremeXOS 11.6 includes all fixes up to and including ExtremeXOS 11.1.4.4, ExtremeXOS 11.2.3.3, ExtremeXOS 11.3.4.5, ExtremeXOS 11.4.4.7, and ExtremeXOS 11.5.2.10. For information on those fixes, see the release notes for the specific release.

General

Assigning a protocol to a VLAN is now working correctly in ExtremeXOS 11.6 (PD3-93519965).

The port LED no longer reverses ports 1 and 2, and ports 3 and 4 on a 10G4Xa module on a BlackDiamond 8800 series switch, and no longer stays amber, with or without traffic (PD3-92086401).

BlackDiamond 8800 Series of Switches

If you apply a policy file with 1,000 rules and counters to ports on the BlackDiamond 8800 a-series and e-series modules and experience multiple MSM failovers, I/O modules and the original primary MSM no longer enter the Failed state (PD3-78583000, PD3-78144707)

MSM I/O ports on the original primary MSM are now available during the failover process. It no longer takes about 2 minutes for these MSM I/O ports to be able to pass traffic again (PD3-48072699).

On a BlackDiamond 8810, deleting a VLAN with OSPF enabled no longer causes the OSPF process to crash (PD3-95772971).

During an MSM failover, there is no longer a reduction in the backplane bandwidth while the original primary MSM reboots (PD3-60905749, PD3-48146450).

BlackDiamond 10808 Switch

On a BlackDiamond 10808 switch running a G20X module, all ports now detect the media (PD3-87860490).

BlackDiamond 12800 Series Switches

RX CRC errors are no longer occurring on a BlackDiamond 12804 after an MSM failover and switch reboot (PD3-91718962).

Traffic queue statistics are now correct when the switch is configured to work in the HQoS mode (PD3-86738591).

The `install firmware` command now upgrades the uC without rebooting the secondary MSM (PD3-92715933, PD3-92095431).

Summit Family of Switches

When a port belongs to another vMAN as an untagged port and you try to add that port again as an untagged member of another vMAN, the `show vman` command no longer generates an error (PD3-45837691).

The wrong error message is no longer generated when a port is an untagged member of vMAN1 and is added to vMAN2 as untagged (PD3-59227575).

After making configuration changes while in shutdown mode, the shutdown prompt is no longer removed, causing it to return to the normal command prompt even though the switch is still in the shutdown state (PD3-77356633).

Summit X450 switches have a 10G and Stack port LED on the front panel. These LEDs are now also included on the Summit X450a-24x switch (PD3-83410991).

On a Summit X450e-24p, ports are no longer deleted from the default VLAN after running the `configure sys-recovery-level switch shutdown` command and without saving the configuration (PD3-91536139).

MAC lockdown timeout entries timeout on continuous traffic when aging time is less than 20 s Seconds (PD3-92939872).

Rebooting a Summit X450 no longer generates errors (PD3-93758236).

An ACL rule that uses an IPv6 source address with a 128-bit prefix and an IPv6 destination addresses with a 128-bit prefix no longer fails (PD3-29697708).

ACL

Enabling IP security using DHCP snooping using the `enable ip-security dhcp-snooping vlan vipsec port all violation-action` command now deletes all ACL entries (PD3-87515636).

CLI

On a BlackDiamond 8810 and a BlackDiamond 10808 switch, an invalid slot ID is no longer displayed in the `show configuration node` command (PD3-92435760, PD3-29753980).

Control Protocols

Disabling ELRP-poll on a specified port no longer disables ELRP on all enabled ports in an ESRP domain (PD3-93043515).

The TX counter no longer increments when ELRP TX packets are sent from a disabled port using the `configure esrp1 elrp-master-poll disable` command (PD3-85845381).

When configuring LLDP, enabling LLDP, and disabling and enabling ports, the "lldp remote table changed" SNMP trap is now sent (PD3-95652242).

Device Management

In a dual MSM BlackDiamond 8800, when the switch is booting up or rebooting, log messages are no longer shown for MSM A and MSM B (PD3-93581660).

DHCP

If you configure a Summit X450 switch as a DHCP server and enable DHCP snooping, the DHCP bindings database is now updated (PD3-95839166).

EAPS

Restarting EAPS process using the `restart process eaps` command no longer causes a loop (PD3-78155331).

When upgrading from ExtremeXOS 11.4.1.4 to ExtremeXOS 11.6, the secondary port is now blocked and no longer causing a traffic loop (PD3-108898932).

In an EAPS domain that belongs to two EAPS shared port instances, with both ring ports configured as shared ports, deleting a shared port does not remove the FDB entries for the other shared port (PD3-61772311).

Errors are no longer generated when running EAPS on multiple domains and one shared link, after deleting the VLANs from the master MSM and reinserting the backup MSM (PD3-74051244).

ESRP

Performing an ESRP state change on a BlackDiamond 8810 or BlackDiamond 10808 no longer generates an error message (PD3-45596286).

Using a Summit X450e-48p, ESRP with RIP no longer generates a RIP coredump when running the `save` and `reboot` commands (PD3-93054015).

After configuring a BlackDiamond 8810 with ESRP and load sharing, once the load sharing port is removed from the switch, the switch master no longer changes (PD3-78083082, PD3-75709097).

FDB error messages are no longer displayed in the log file during ESRP flaps when enabling and disabling ESRP (PD3-86435357).

IP Routing Protocols

On a Summit X450a-48 switch, once Duplicate Address Detection is detected, IPv6 switching no longer stops even after the duplicate address is removed (PD3-91597373).

During scaling testing with more than 1,000 routes, if the next hop is a link local address that is not resolved at the time the route is installed, forwarding no longer shifts from the hardware to the software path (PD3-99598191, PD3-99081628).

IPv6 Multicast

After you enable router discovery on a VLAN, if you issue the `show configuration` command, the values for the minimum time between sending unsolicited router advertisements and the default lifetime are now displayed correctly (PD3-78133211).

MPLS

Running an MSM failover on a redundant BlackDiamond 12804 switch, the virtual private LAN services sessions between the BlackDiamond 12804 switches no longer gets stuck in SGNL state (PD3-93332451).

When configuring an ingress LSP to a neighbor LSR ID and then configuring the LSP to the DUT on the neighbor LSR, the HELLO, PATH_ERR, and RESV messages are no longer MPLS encapsulated using the label advertised for the ingress LSP DUT (PD3-92652799).

To enable LDP to advertise a label mapping for the LSR ID, configure a loopback VLAN with an IP address equal to the LSR ID and issue the `configure mpls ldp advertise direct lsr-id` command (PD3-92652381).

Pseudo wire vMAN service packets are no longer forwarded by the CPU on MPLS transit switches if the service packets are connected using tagged ports (PD3-82141781).

Clearing an FDB on a master MSM no longer displays an error message on the slave MSM console (PD3-85911101).

VPLS-enabled VLANs can now be VPLS-enabled after the MPLS process is restarted (PD3-84697051).

Multicast

Multicast switching now works properly after issuing the `clear igmp snooping` command (PD3-94768228).

Proxy IGMP report and leave messages are now sent with the correct VLAN tag by a tagged MVR VLAN (PD3-78255021).

When configuring routing on a BlackDiamond 8800 or Summit X450 switch to a multicast MAC address with multiple ports, multicast now forwards the packets (PD3-48186431).

Network Login

The reauthorization period range displayed in the output of the `configure netlogin dot1x timers reauth-period` command is now correct (PD3-73555765).

A device that is configured for web-based Network Login (campus mode) and the RADIUS server sends an access-accept message to the device after user verification, no longer sends a 401 unauthorized message to the client PC (PD3-84009271)

When multiple supplicant authentications are sent through a single port, authentication is now working properly when enabling a dynamic VLAN configuration (PD3-93649841).

Network Services

The `clear igmp group` command no longer clears statically configured IGMP receivers and the dynamic receivers (PD3-75790312).

Adding a third port to a static link aggregation trunk no longer generates an error message (PD3-74850381).

After creating and enabling a VLAN with a load-sharing group, and then enabling a jumbo frame, traffic is now forwarded over the load-sharing group (PD3-46068593).

Network Tools

The built-in BOOTP client now recognizes BOOTREPLY packets (PD3-73957069).

Security

If you configure a Summit X450 switch as a DHCP server and enable source IP lockdown, the default ACL to allow traffic is now created and the DHCP bindings database is now updated. If you enable BOOTP relay and source IP lockdown on a Summit X450 switch, the default ACL to allow traffic is now created (PD3-95842403).

Rapid Spanning Tree Protocol

Splitting a VLAN over multiple RSTP domains no longer causes a potential loop (PD3-89661191).

Spanning Tree Protocol

The CLI will not allow configuring MSTI domains with same ID (PD3-84750478, PD3-75926621).

Configuring MSTP and other STP protocols such as STP, RSTP, EMISTP on the same physical port, MSTP and other STP protocols now function correctly (PD3-84750814, PD3-60166873).

When MSTI is disabled, the `show msti ports` command now displays the port state as forwarding, not disabled (PD3-84750557, PD3-75032891).

When changing Operational mode from dot1d to dot1w, the topology change flag turns off (PD3-77357141).

On Summit X450 platforms, traps are now generated when edge ports move to the blocked state after receiving bpdus (PD3-73988838).

