ExtremeXOS Release Notes

Software Version ExtremeXOS 15.3.5-Patch1-3

Published May 2015
120851-00 Rev 22

Legal Notices

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

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

Trademarks

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

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

For additional information about Extreme Networks trademarks, go to: www.extremenetworks.com/company/legal/trademarks/

Support

For product support, including documentation, visit: www.extremenetworks.com/support/

Contact

Extreme Networks, Inc.
145 Rio Robles
San Jose, CA 19534
Tel: +1 408-579-2800
Toll-free: +1 888-257-3000

Table of Contents

1 Overview

These release notes document ExtremeXOS® 15.3.5-Patch1-3 which resolves software deficiencies.

This chapter contains the following sections:

New and Corrected Features in ExtremeXOS 15.3.2

This section lists the feature corrections supported in ExtremeXOS 15.3.2 software:

Protocol Independent Multicast (PIM) Designated Router (DR) Priority

The DR_Priority option allows you to prioritize a particular router in the DR election process by assigning it a numerically larger DR Priority. Every Hello message includes the DR_Priority option, even if no DR Priority is explicitly configured on that interface. This is necessary because priority-based DR election is only enabled when all neighbors on an interface advertise that they are capable of using the DR_Priority Option. The default priority is 1.

DR Priority is a 32-bit unsigned number, and the numerically larger priority is always preferred. A router's idea of the current DR on an interface can change when a PIM Hello message is received, when a neighbor times out, or when a router's own DR Priority changes. If the router becomes the DR or ceases to be the DR, this normally causes

the DR Register state machine to change state. Subsequent actions are determined by that state machine.

The DR election process on the interface consists of the following:

- If any one of the neighbors on the interface is not advertised, the DR priority (not DR capable) is not considered for the all the neighbors in the circuit and the primary IP address is considered for all the neighbors.
- Higher DR priority or higher primary address is elected as DR.

Changed CLI Command

Changes are bolded.

`configure pim {ipv4 | ipv6} [ {vlan} <vlan_name> | vlan all ]` **`dr-priority <priority>`**

The output of the `show pim` and `show pim ipv6` commands now displays the DR Priority.

MAC Address Hash

The hash algorithm used for the L2 MAC hash table has been improved so that more MAC addresses can be inserted prior to filling the hash bucket.

This feature applies only to the Summit X670, BlackDiamond 8900-40G6Xc, and BlackDiamond X8 series switches.

VMAN Double Tag

The VMAN double tag feature adds an optional port CVID parameter to the existing untagged VMAN port configuration. When present, any untagged packet received on the port is double tagged with the configured port CVID and SVID associated with the VMAN. Packets received with a single CVID on the same port still have the SVID added. As double tagged packets are received from tagged VMAN ports and are forwarded to untagged VMAN ports, the SVID associated with the VMAN is stripped. Additionally, the CVID associated with the configured Port CVID is also stripped in the same operation. CVIDs that do not match the configured port CVID are not stripped on the same port.

Much like the CVIDs configured as part of the CEP feature, the configured Port CVID is not represented by a VLAN within ExtremeXOS. The implication is that protocols and individual services cannot be applied to the port CVID alone. Protocols and services are instead applied to the VMAN and/or port as the VMAN represents the

true layer 2 broadcast domain. Much like regular untagged VMAN ports, MAC FDB learning occurs on the VMAN, so duplicate MAC addresses received on multiple CVIDs that are mapped to the same VMAN can be problematic. Even when the additional Port CVID is configured, the port still has all of the attributes of a regular untagged VMAN port. This means that any single c-tagged packets received on the same port have just the SVID associated with the VMAN added to the packet. Likewise, any egress packet with a CVID other than the configured Port CVID will have the SVID stripped.

Limitations

Any limitations that currently exist with untagged VMAN ports also exist when the Port VLAN ID element is additionally applied.

Supported Platforms

All Summit, BlackDiamond 8800, and BlackDiamond X8 platforms are supported, except the following:

- Summit X150, X250e, X350, X450e, X450a
- BlackDiamond 8800: G48Te2, G24Xc, G48Xc, G48Tc, 10G4Xc, 10G8Xc, S-G8Xc, S-10G1Xc, S-10G2Xc
- BlackDiamond 8800: 8500-series

Changed CLI Commands

Changes are bolded.

`config vman <vman-nMame> add ports [<port_list> | all] untagged` **{port-cvid <port_cvid>}**

The output of the `show vman <vlan_name> | detail` command now displays the port CVID.

STP Instances Scale Fix

The STP Instances Scale fix resolves a software deficiency (see PD4-3427549640 in the Resolved Issues in ExtremeXOS 15.3.2 on page 143) and increases limit values (see below table).

Table 1: Supported Limits

Metric	Product	Limit
Spanning Tree PVST+—maximum number of port mode PVST domains. **NOTE:** • Maximum of 10 active ports per PVST domain when 256 PVST domains are configured. • Maximum of 7 active ports per PVST domain when 128 PVST domains are configured.	BlackDiamond X8 and 8900 series switches Summit X670 Summit X460, X480, X650, X440	256 256 128
Spanning Tree (number of ports)—maximum number of ports including all Spanning Tree domains.	All platforms	4,096

For a complete list of supported limits, see Supported Limits on page 51.

Increase Protocol Independent Multicast (PIM) Neighbors in Advanced Edge License.

This feature expands the number of PIM neighbors in our Advanced Edge license from two to four.

Change Default Parameter for Protocol Independent Multicast (PIM)-Register-Checksum Command

This feature changes the default parameter for the `configure pim register-checksum-to` command to be the RFC method which would be the following: `configure pim register-checksum-to exclude-data`.

Lawful Intercept

If you have lawful Intercept user privileges, you can log in to a session and configure lawful intercept on the switch. The configuration consists of dynamic ACLs and a mirror-to port to direct traffic to a separate device for analysis. The lawful intercept logon session, session-related events, and the ACLs and mirror instance are not visible to, or modifiable by, any other user (administrative or otherwise).

No lawful intercept configuration is saved in the configuration file, and it must be reconfigured in the case of a system reboot.

Other important feature information:

- An administrative user can create and delete a single local account having the lawful intercept privilege but not the write privilege, and can set its initial password.
- The lawful intercept user is required to change the password (for the single lawful intercept-privileged account) upon logging on for the first time. An administrative user can delete the lawful intercept account.
- The password for the lawful intercept account can only be changed by the lawful intercept user and cannot be changed by an administrative user.
- The `show accounts` command displays the existence of the lawful intercept account, but does not display any related statistics.
- The `show configuration` command does not display the lawful intercept account.
- The `show session {detail | history}` command does not display any lawful intercept user information. The EMS events normally associated with logging on and off are suppressed, and do not occur relative to logging on and off of the lawful intercept account.
- The EMS events normally associated with the `enable cli-config-logging` command are suppressed, and do not occur relative to a lawful intercept user session.
- The lawful intercept user can create and delete non-permanent dynamic ACLs with the mirror action only. The lawful intercept user cannot create or delete any other ACLs.
- The `show access-list` command does not display any lawful intercept user-created ACLs to a non-lawful intercept user.
- The lawful intercept user-created ACLs are not accessible for any use by a non-lawful intercept user (specifically through the `configure access-list add` or `configure access-list delete` commands).

- The lawful intercept user can only create or delete one (non-permanent) mirror instance with which to bind the lawful intercept user-created ACLs and specify the mirror-to port.

Changed CLI Commands

Changes are bolded.

```
create account [user | admin | lawful-intercept] <account-name>
{encrypted} {<password>}

show mirror {<mirror_name> | <mirror_name_li> | all | enabled | summary}

show access-list dynamic {rule [<rule> | <rule_li>]}

show access-list dynamic rule [<rule> | <rule_li>] detail
```

NOTE

The new arguments `<mirror_name_li>` and `<rule_li>` are only be available if the user is logged on to the lawful intercept account.

The output of the `show accounts` command now displays lawful intercept user information if you are logged on as a lawful intercept user.

IGMP and MLD Loopback

This section explains the new feature, IGMP and MLD loopback, which allows configuration of static and dynamic groups on a VLAN without specifying a portlist. The traffic is pulled from upstream, but not forwarded to any port. The loopback (Lpbk) port is a logical port on a VLAN in the application context. When you configure a group on a VLAN, but do not specify the port, the switch forms an IGMPv2/MLDv1 join and assumes it to be received on Lpbk port. A dynamic group ages out after the membership timeout, if there are no other receivers. Membership joins refresh the dynamic group. The static group stays until it is removed from the configuration.

Limitations

- If the VLAN is not in loopback mode, at least one port should be up for the command(s) to take effect.
- In an MLAG setup, configure the command(s) on both MLAG peers, if the intention is to create or delete a receiver on the MLAG port.

Supported Platforms

- All Summit family switches
- BlackDiamond 8800 series switches with master switch fabric modules (MSMs) supported for the ExtremeXOS 15.3.2 release
- BlackDiamond X8 series switches

CLI Commands

Configure Dynamic Groups (New Command)

```
configure [igmp | mld] snooping {vlan} <vlan_name> {ports <portlist>}
add dynamic group [ <v4Group> | <v6Group> ]
```

NOTE

This command is not saved in the configuration.

Add Static Groups

```
configure igmp snooping {vlan} <vlan_name> {ports <portlist>} add
static group <ip_address>
```

```
configure mld snooping {vlan} <vlan_name> {ports <portlist>} add
static group <ip_address>
```

Delete Static Group/All Groups

```
configure igmp snooping {vlan} <vlan_name> {ports <portlist>} delete
static group [<ip_address> | all]
```

```
configure mld snooping {vlan} <vlan_name> {ports <portlist>} delete
static group [<ip_address> | all]
```

When the `all` option is used, but portlist is not specified, only the groups configured for Lpbk port are deleted. You should use the `portlist` option to delete the groups configured for specific ports.

Commands Modified to Display Port as Lpbk

The outputs of the following commands now display port as “Lpbk,” when portlist is not configured:

```
show [igmp group {<grpipaddress> | {vlan} {<name>}} {IGMPv3} | mld
group {<v6grpipaddress> | {vlan} {<name>}} {MLDv2}]

show igmp snooping [detail | {vlan} <name> {port <port>}] {IGMPv3}

show mld snooping [detail | {vlan} <name>] {MLDv2}

show igmp snooping {vlan} <name> static group

show mld snooping {vlan} <name> static group

show [ mvr cache {{vlan} <vlan-name>}  | igmp snooping cache {{vlan}
<name>} { group <grpaddressMask> | <grpaddressMask>} {with-in-port} |
mcast {ipv4} cache {{vlan} <name>} { { [group <grpaddressMask> |
<grpaddressMask> | <grpAddr> ]  {source <sourceIP> | <sourceIP> }} {
type [snooping | pim | mvr] } {with-in-port} | {summary} } | mcast
ipv6 cache {{vlan} <name>} { { [group <v6GrpAddressMask> |
<v6GrpAddressMask> | <v6GrpAddr> ]  {source <v6SourceIP> |
<v6SourceIP> }} { type [snooping | pim ] } {with-in-port} | {summary}
} ]
```

Multicast Equal Cost Multipath (ECMP) Feature

The Multicast Equal Cost Multipath (ECMP) feature supports PIM routers to load split traffic over different equal cost multiple paths instead of sending all traffic over a single path.

NOTE:

This feature does load splitting and not load balancing.

Limitations

- PIM can support a maximum of 32 ECMP paths.
- Cannot be used along with static multicast routes.
- Not supported for ExtremeXOS Multicast Tools (mtrace and mrinfo) in current release.
- Load splitting is not applied for multicast routes in the multicast routing table.
- Load splitting is only effective when the equal cost paths are upstream PIM neighbors on different interfaces. When the equal cost paths are PIM neighbors on the same shared VLAN, PIM assert mechanism chooses one path to avoid traffic duplication. The path chosen by PIM assert mechanism overrides the path selected by Multicast ECMP load splitting.

Supported Platforms

All platforms, except the Summit X440 series switches.

CLI Commands

This command is used to enable or disable the Multicast ECMP feature. This variable cannot be changed when PIM is enabled.

```
[enable | disable] pim {ipv4 | ipv6} iproute sharing
```

This command is used to configure PIM ECMP hash algorithm. The value cannot be changed when PIM and PIM-ECMP are enabled.

```
configure pim {ipv4 | ipv6} iproute sharing hash [source | group |
source-group | source-group-nexthop]
```

Error Messages

PIM route sharing cannot be enabled or disabled when PIM is already enabled. PIM route sharing hash also cannot be modified when PIM route sharing and PIM are already enabled, so the following error message appears when you try to execute these commands:

Error message for IPv4:

```
Error: This command cannot be executed when PIM is enabled. Disable
PIM using "disable pim" command and try again.
```

Error message for IPv6:

```
Error: This command cannot be executed when PIM is enabled. Disable
PIM using "disable pim ipv6" command and try again.
```

Bidirectional Forwarding Detection (BFD)

BFD (Bidirectional Forwarding Detection) is an ExtremeXOS service that provides rapid failure detection of the forwarding path to a next-hop, and sends failure detection notices to its clients (for example, routing protocols) to initiate recovery action.

Limitations

- Process restart may cause BFD state loss.
- BFD parameters are configured on a per interfaces basis, instead of per next-hop basis.
- ExtremeXOS BFD limitations are inherited.
- No hardware-supported BFD.

BFD for Open Shortest Path First (OSPF) v2/v3

Without BFD, OSPF detects failures based on OSPF timers, which are not as granular as BFD timers.

Modified CLI Commands for OSPF v2/v3

Changes are in bold:

```
show bfd session client [mpls | ospf | static] {ipv4 | ipv6} {vr
[<vrname> | all]}
```

For OSPF interfaces commands, there is a new flag “b” to represent BFD protection configuration.

For OSPF neighbor commands, the BFD session state now appears on display states and error messages:

- None—BFD session is not requested.
- Active—BFD session is successfully created and is in UP state.
- Disabled—BFD session is in Admin Down state.
- Pending—BFD session request is pending on response from server.
- Error (Session Limit Exceeded), Error (Out of Memory), Error (Connection Lost), Error (Communication Failure), Error (BFD Internal Error).

`show ospf memory` includes memory statistics for ospfBfdSess.

`show ospfv3 memory` includes memory statistics for BfdSess.

When OSPF is disabled on one or all VLANs (router interfaces) using the following commands:

```
configure ospf delete vlan [<vlan-name> | all]
```

```
configure ospfv3 delete vlan [<vlan-name> | all]
```

BFD for OSPF configuration is removed from those interfaces as well, and OSPF requests the BFD sever to delete all BFD sessions created on those interfaces.

The “unconfigure” commands:

```
unconfigure ospf {vlan <vlan-name> | area <area-id>}
```

```
unconfigure ospfv3 {vlan <vlan-name> | area <area-id>}
```

also reset the BFD configuration to the default setting “off” on one or all OSPF interfaces. Requests are sent to BFD server to delete all BFD sessions for those OSPF interfaces.

When router OSPF is disabled using the following commands:

```
disable ospf
```

```
disable ospfv3
```

BFD for OSPF configuration is removed as well, and OSPF requests the BFD sever to delete all BFD sessions.

New CLI Commands for OSPF v2

```
configure ospf {vlan} <vlan-name> bfd [on | off]
```

New CLI Commands for OSPF v3

```
configure ospfv3 {domain <domainName>} {vlan} <vlan-name> bfd [on |
off]
```

BFD for IPV6 Static Routes

BFD OSPF protocol now supports IPv6 for single-hop sessions. This allows Route Manager to use BFD liveness protection capabilities to help determine the operational state of IPv6 static routes.

New CLI Commands

```
enable iproute bfd {gateway} [<ip_addr> | <ipv6Gateway>] {vr <vrname>}

disable iproute bfd {gateway} [<ip_addr> | <ipv6Gateway>] {vr
<vrname>}
```

Modified CLI Commands

Changes are in bold.

```
configure iproute add <ipv6Netmask> [ <ipv6Gateway> {bfd} |
<ipv6ScopedGateway> ] {<metric>} { {unicast | multicast } {vr
<vrname>} | {vr <vrname>} { unicast-only | multicast-only} }

configure iproute add default [ <ipv6Gateway> {bfd} |
<ipv6ScopedGateway> ] {<metric>} { {unicast | multicast } {vr
<vrname>} | {vr <vrname>} { unicast-only | multicast-only} }
```

Specifying the “bfd” keyword when adding a static route explicitly defines the route to be protected by the BFD session to the nexthop neighbor (gateway). Subsequently, the operational status of the route reflects the operational status of the BFD session when the session is enabled and current. If the BFD session is disabled or continues in the INIT state, then the operational state of the BFD session is not considered in determining the operational state of the route.

```
show iproute bfd { {ipv4} <ip_addr> | ipv6 {<ipv6Gateway>} } { vr [all |
<vrname>] }
```

This command is expanded to display the current BFD session state of all Route Manager nexthop IPv6 neighbors that have been configured as BFD enabled. The output includes a count of associated static routes that have been configured as BFD protected (source direction only).

Possible BFD session states: active (up), active (down), pending, disabled, error (session limit exceeded), error (out of memory), error (connection lost), error (communication failure), error (BFD internal error).

`show iproute bfd ipv6`

The output of the `show iproute bfd ipv6` has been modified by the addition of two new flags:

- **b**—route is configured for BFD protection, but protection is not yet active.
- **p**—route has active BFD protection.

`show iproute bfd`

The output of `show iproute bfd` for IPv4 nexthop neighbors is modified to be consistent with IPv6 format.

Possible BFD session states: active (up), active (down), pending, disabled, error (session limit exceeded), error (out of memory), error (connection lost), error (communication failure), error (BFD internal error).

New Hardware Supported in ExtremeXOS 15.3.2

This section lists the new hardware supported in ExtremeXOS 15.3.2:

- Summit X430
  - Summit X430-24t
  - Summit X430-48t

NOTE:

Summit X430 series switches require a different ExtremeXOS file than other Extreme Network Summit switches. The required file is “summitlite-15.3.2.11.xos”.

New Features and Functionality in ExtremeXOS 15.3

ExtremeXOS 15.3 includes the following features:

Multiple Stream Registration Protocol (MSRP) for Audio Video Bridging (AVB)

Stream Reservation Protocol (SRP) enables bandwidth reservation for data streams from a talker end-station to one or more listener end-station(s) for Audio Video Bridging (AVB). SRP uses three MRP-based protocols to complete the end-to-end reservation. MVRP adds the ports to the VLAN where the data stream resides, MMRP optionally learns the listeners that are interested in the data streams, and MSRP reserves bandwidth for the stream. MSRP in turn uses Forwarding and Queuing for Time-Sensitive Streams (FQTSS) to manage scheduling.

This feature includes:

- Support for SRP in accordance with IEEE 802.1Qat-2010 including support for:
  - IEEE 802.1Qat-2010 MSRP
  - IEEE 802.1Qav-2009 Forwarding and Queuing for Time-Sensitive Streams (FQTSS)
- Declaration and registration of MSRP domain discovery and reservation
- Reserve link capacity for the user of SRP streams

Limitations

- Stacking is not supported.
- IEEE8021-SRP-MIB is not currently supported.
- Talker pruning is not available, since MMRP is not available.
- 802.11 designated MSRP node (DMN) support is not available.
- LAG and MLAG are not supported.
- The only supported layer 2 topology protocols are STP and RSTP. In particular, MSTP, EAPS, and ERPS are not supported, and MVRP/MSRP should not be enabled on the same ports as MSRP, EAPS or ERPS.
- When using AVB with STP or RSTP, VLAN “default” must be the carrier VLAN for the STP domain on the ports where AVB is enabled.
- Maximum number of active streams:
  - For the Summit X440 and X460: 1024.
  - For the Summit X670: 8,192.

Supported Platforms

- Summit X460 series switches
- Summit X670/X670V series switches
- Summit X440 series switches

Multiple Registration Protocol (MRP)/Multiple VLAN Registration Protocol (MVRP)

Multiple Registration Protocol (MRP) is a simple, fully distributed, many-to-many protocol, that supports efficient, reliable, and rapid declaration and registration of attributes by multiple participants on shared and virtual shared media. MRP allows a participant of a given MRP application to make or withdraw declarations of attributes, which results in registration of those attributes with the other MRP participants for that application. MRP does not do any work on its own, but rather provides the framework and state machines for implementing MRP applications such as Multiple VLAN Registration Protocol (MVRP), Multiple MAC Registration Protocol (MMRP), and Multiple Stream Registration Protocol (MSRP).

This feature includes:

- MRP and MVRP implementation as per IEEE 802.1ak-2007
- Support for Secure Remote Password Protocol (SRP) for Audio Video Bridging (AVB)
- Support for XNV Dynamic VLAN propagation
- Support IDM role-based VLAN propagation
- Support for MVRP over individual Ethernet ports

Limitations

- MIB support is not available.
- MVRP support for EAPS is not available.
- MVRP over MLAG is not available.
- MMRP (part of IEEE 802.1ak-2007) is not supported.
- VMAN (S-VLAN) creation is not available.

Multi-protocol Label Switching (MPLS) Layer 3 Virtual Private Network (L3 VPN)

L3 VPNs provide the ability to interconnect IP networks across a shared MPLS BGP backbone. Networks interconnected using the same provider edge (PE) device may have overlapping IP addresses. Customer-specific IP addresses are separately managed using unique Virtual Routing and Forwarding (VRF) domains. Each VRF instance maintains a separate IGP topology and separate routing tables associated with each customer. This is also commonly referred to as light-weight L3 VRs.

This feature includes:

- Multiple VRF support
- Multi-instance (RIB) BGP protocol
- VPN-IPv4 address family support in BGP
- BGP carrying labeled VPN-IPv4 routes
- BGP for PE–CE peering routing protocol
- Static routes per VRF
- Two layer MPLS label stack for data traffic forwarding
- Ping and Traceroute network diagnostics tools under a VPN scope
- SNMP support to control and monitor parameters of all VR/VRFs
- BGP/MPLS VPN MIB access (read only), as per RFC-4382 (except two tables)
- OSPFv2 and ISIS as core (SP's backbone) IGP routing protocol
- RFC 1657 MIB support

Limitations

The following are not supported:

- Static L3VPN
- RIP for PE–CE peering routing protocol
- IP Multicast BGP/MPLS VPN
- OSPFv2 and ISIS for PE–CE peering routing protocol
- IPv6 VPN
- Graceful restart mechanism for BGP with MPLS (RFC-4781)
- Constraint Route distribution for BGP/MPLS VPN (RFC-4684)
- Carrier of carriers BGP/MPLS VPN configuration (RFC 4364, Section 9)

- XML support to configure BGP/MPLS VPN parameters
- VR/VRF Management Account
- BGP Outbound Route Filtering (ORF)
- Inter-AS/inter-provider VPNs (RFC 4364, Section 10)
- Route leaking of internet default routes into the VRFs
- BGP-related MIBs, other than RFC 1657

Supported Platforms

MPLS L3 VPN feature is supported on all platforms that can support MPLS L3 VPNs:

- Summit X480 series switches
- Summit X460 series switches
- Summit X670 series switches
- BlackDiamond 8800 series switches with XL modules
- BlackDiamond X8 series switches
- E4G-200 and E4G-400 cell site routers

Network Time Protocol (NTP)-Virtual Router Redundancy Protocol (VRRP) Virtual IP

This feature adds the ability for switches to configure the Virtual Router Redundancy Protocol (VRRP) virtual IP as a Network Time Protocol (NTP) server address. The NTP server when configured on the VRRP master monitors the physical and virtual IP address for NTP clients.

Requirements

- For this feature to work correctly, you need to enable “accept” mode in VRRP using the following command:

  ```
  configure vrrp vlan <vlan_name> vrid <vridval> accept-mode [on | off]
  ```

  Enabling accept mode allows the switch to process non-ping packets that have destination IP set to the virtual IP address.

- Summit switches configured as NTP clients need to have the following bootrom version:
  - Summit X480, X460, X440, X670: 2.0.1.7
  - Summit X150,250e, X350, X450a, X450e, X650, NWI-E450A:1.0.5.7

- The use of FHRP Virtual IPs is usually not recommended for NTP configuration since it can cause undesirable behavior when the NTP servers themselves are not in sync or if the delay is asymmetric. Therefore, ensure that both servers derive their clock information from the same source.

  The problem may be more acute if there is a node connected to VRRP peers using MLAG and VRRP is in active-active mode. In this case, there is a theoretical possibility that every other packet can be sent to a different switch due to LAG hashing at the remote node.

Port Isolation

This feature blocks accidental and intentional inter-communication between different customers residing on different physical ports. Previously, this kind of security was obtained through the access-list module, but this can be complicated to manage and can be resource intensive. This feature provides a much simpler, more elegant, blocking mechanism without the use of ACL hardware.

You select a set of physical ports or load share ports which are deemed isolated. Once a physical port or load share port is isolated, it cannot communicate with other isolated ports, but can communicate with any other port in the system.

Blocked traffic types include:

- L2 unicast
- L2 multicast
- L2 unknown unicast
- L2 broadcast,
- L3 unicast
- L3 multicast

New CLI Command

The following command is available to enable isolation mode on a per-port basis (default = off):

```
configure ports <port_list> isolation [on | off]
```

The above command can be issued either on a single port or on a master port of a load share group. If the command is issued on a non-master port of a load share group, the command fails. When a port load share group is formed, all of the member ports assume the same ‘isolation’ setting as the master port.

Limitations

Port isolation is not allowed on the mirror-to port.

Supported Platforms

- BlackDiamond X8 series switches
- BlackDiamond 8800 series switches
- All Summit family switches

Ethernet Ring Protection Switching (ERPS) G.8032 Enhancements

The basic concept of G.8032/ERPS is that traffic may flow on all links of a ring network except on one link called the Ring Protection Link (RPL). The RPL owner is the node that blocks the RPL and the other node of the RPL is called the RPL neighbor node. All other nodes are called non-RPL nodes. When a link fails, the RPL owner unblocks the RPL to allow connectivity to the nodes in the ring. The G.8032/ERPS rings uses a channel (dedicated path) for carrying their control traffic which is the R-APS messages.

The following enhancements have been added to the ERPS feature in ExtremeXOS:

- G.8032 version 2 with “no virtual channel support”
- Support for attaching to a Connectivity Fault Management (CFM) down-maintenance end point (MEP) configured external to ERPS
- Multiple failure protection for subrings using up-MEP (as per Appendix X.3 of G.8032 standard)

Limitations

- Backup master switch fabric module (MSM) failover and checkpointing for both v1 and v2 not available.
- In platforms that do not have hardware OAM, the recommended CFM interval is 1 second for link monitoring, which produces approximately 3 seconds of overhead in convergence times.
- Optimizations done in EAPS for Virtual Private LAN Service (VPLS) and any other within EAPS are not available.
- No interoperability with Spanning Tree Protocol (STP).
- Simple Network Management Protocol (SNMP) is not available.

ExtremeXOS Network Virtualization (XNV) Per Virtual Machine (VM) Statistics

For ExtremeXOS 15.3, per virtual machine (VM), for each direction, you can install counters to count ingress and egress traffic using the command:

```
configure vm-tracking vpp <vpp_name> counters [ingress-only | egress-only | both | none]
```

- For each local and network VPP, you can now specify whether counters need to be installed to count traffic matching VM MAC, which gets this VPP mapping.
- You can collect statistics on ingress traffic, egress traffic, or both. You can disable counters at any time.
- You can view the list of packets/bytes counts of this counter using CLI command `show access dynamic-counter`.
- The counter is un-installed when the VM MAC is deleted on the switch or VPP gets mapped to the VM MAC, or the counter option is set to none.
- If the VM MAC move happens, then the counter installed on previous port is un-installed and the counter is installed on new port. The counter values of old port are not maintained during the MAC move.

Limitations

During VM MAC moves, the values dynamic counters installed on the previous port are not maintained.

Ethernet Automatic Protection Switching (EAPS) License Change

The Ethernet Automatic Protection Switching (EAPS) (multiple rings with multiple interconnect points, no shared-ports) feature is now part of the Advanced Edge license option, rather than the Core license option.

Identity Management (IDM) OR Operation and Active Directory (AD) Group Attribute Support

ExtremeXOS now supports the following enhancements to Identity Management (IDM):

- OR operation in match criteria of user roles.

  Previously, ExtremeXOS supported only AND in the match criteria of user roles. Now OR is also supported—the user can have either AND or OR in the match criteria, but not both. That is, for a particular role, you can have all match criteria with AND, or have all the match criteria with OR. For role hierarchy and match criteria inheritance, there is no restriction across roles. You can have the parent role with AND, and the child role with OR, or vice versa. The inheritance of match criteria to the child role from the parent uses AND.

- Added support for Lightweight Directory Access Protocol (LDAP) group attributes.

  Network users can be mapped to a role based on group membership (distribution list) information. When a user is detected by identity manager, it retrieves the groups that the detected user is member of from LDAP server. Identity manager then places the user under the appropriate role, based on group information and existing 8 LDAP attributes as supported today.

Limitations

Mix of AND and OR is not supported in the match criteria definition of the role.

IPv6 Equal-Cost Multi-Path (ECMP)

This feature adds IPv6 Equal-Cost Multi-Path (ECMP) support. Also, support is added for 16-way and 32-way ECMP for both IPv4 and IPv6, using static routes. Previous releases were limited to 2, 4, or 8-way ECMP.

Sharing of ECMP gateway sets now applies to IPv6 as well as IPv4. Sharing of ECMP gateway sets for IPv6 means the entire IPv6 Longest-Prefix Match (LPM) hardware capacity can use ECMP, across up to 32 gateways.

Supported Platforms

- Summit X460, X480, X650, X670 (stack or standalone)
- E4G-200, E4G-400 cell site routers
- BlackDiamond 8800 series switches with all I/O modules
- BlackDiamond X8 with all I/O modules

CLI Commands

The CLI command to enable/disable IPv6 ECMP is:

```
[enable | disable] iproute ipv6 sharing {{{vr} <vrname>} | { {vr}
all}}
```

The existing CLI command to configure the maximum number of gateways in each IPv4 or IPv6 gateway set now accepts 16 and 32 as acceptable values, along with 2, 4 and 8. As in prior releases, changing the value of max-gateways requires a save and reboot.

```
configure iproute sharing max-gateways <max_gateways>
```

Protocol Independent Multi-cast (PIM) IPv6

This feature provides Protocol Independent Multicast (PIM) support for IPv6. PIM is the de-facto standard for routing multicast traffic over the Internet.

PIM has two types, sparse and dense mode, meant for deployment in different topologies. These two flavors, called PIM-SM and PIM-DM, are entirely different in operation. PIM-SM is an explicit join protocol, where traffic is not forwarded on a segment, unless explicit an request come from the network segment (typically through IGMP). In contrast, PIM-DM is based on the flood-and-prune mechanism, where everybody receives the traffic until they explicitly inform (through PIM-DM prune mechanism) that they don't want to receive that particular stream. Thus, PIM-DM is mainly meant for topologies where listeners are very densely populated. PIM-SM should be deployed where the receivers are sparsely populated over the network, so that most of the network segments' bandwidth is conserved.

This new feature includes support for:

- Secondary address list

  This is added to the V6 hello messages sent. The list includes all addresses assigned to an interface, including the link local addresses. The receiving router must process these addresses and must associate them with the neighbor that sent the message.

- Tunnel interface

  This is very similar to a VLAN interface. You now receive IP address configuration for a tunnel, etc., from the VLAN manager client.

Limitations

The following features are not available:

- Embedded RP support
- Anycast RP support

Link Aggregation Group (LAG) Scaling Enhancements

For *BlackDiamond X8 series switches*: Load sharing groups configured for more than 16 aggregator ports per group no longer need the address-based "custom" algorithm.

For *Summit X670 family switches*: For Summit X670s in a stack, the maximum number of ports per group is increased from 8 to 64.

Limitations

- For Summit X670 switches and X670 stacking, load sharing groups configured for more than 16 aggregator ports per group must use the address-based "custom" algorithm.
- For Summit X670 stacking, all nodes in the stack must be Summit X670s if more than eightaggregator ports per group are configured. For existing configuration with a LAG with more than eight ports, any new non-X670 node added to the stack causes an EMS error.
- With Distributed ARP mode on, the maximum number of aggregator ports on BDX is limited to 16.

Service Verification Tool

This features provides a test tool for operators to verify a new service instance prior to turning the service over to their customers.

CLI Commands

- `run esvt traffic-test {vlan} <vlan_name> loopback-port <loopback-port> peer-switch-ip <ipaddress> packet-size <packet_size> rate <rate> [Kbps|Mbps | Gbps] duration <time> [seconds | minutes | hours]`
- `stop esvt traffic-test {{vlan} <vlan_name>}`
- `show esvt traffic-test {{vlan} <vlan_name>}`
- `clear esvt traffic-test {{vlan} <vlan_name>}`

Limitations

- The service verification tool can be used to verify L2 services only and test network must not cross L2 boundaries.
- One loopback port needs to be assigned for each L2 service test.
- All L2/L3 protocols for the service VLAN should be disabled unless specifically included in the test tool instructions.
- Only modules that support egress ACLs are supported in stacking (BlackDiamond 8800 series switches).
- Remote switch must be an Extreme Networks switch, or a switch that does not generate ICMP errors, and packets are L3 routed within the same VLAN.
- Only one test per VLAN can be actively running.

Supported Platforms

- Summit X460 switches
- Summit X480 switches
- Summit X670 switches
- Summit X650 switches
- SummitStacks with X460, X480, X670, and X650 switches
- E4G-200 and E4G-400 cell site routers
- BlackDiamond 8800 series switches

OpenFlow

NOTE

Currently, OpenFlow does not work in ExtremeXOS Release 15.3.3. OpenFlow does work in ExtremeXOS Release 15.3.1.

The OpenFlow feature enables an external OpenFlow Controller to manipulate data flows within an Extreme Networks switch using a standard protocol to dynamically configure a flow table abstraction. Flow table entries consist of a set of packet matching criteria (L2, L3, and L4 packet headers), a set of actions associated with a flow (flood, modify, forward, divert to controller, etc.), and a set of per flow packet and byte counters. Flow table entries are implemented using hardware ACLs.

Feature highlights:

- Supports line-rate implementation of the OpenFlow flow table by instantiating the flow table in hardware lookup tables.
- Provides the ability for multiple OpenFlow controllers to be configured, with automatic failover to the alternative controller if connectivity is lost with the currently active one.
- Provides the ability for particular ports and VLANs to be configured for OpenFlow control. A particular port can support OpenFlow-managed and non-OpenFlow managed VLANs. Currently, OpenFlow only supports a single VLAN.

NOTE

OpenFlow, XNV, and IDM are all features that enable an external agent to control resources on a switch. Due to their interaction models and resource requirements, these features are mutually exclusive. The ExtremeXOS 15.3 OpenFlow implementation prevents these services from being simultaneously configured on the same port.

CLI Commands

- `[enable | disable] openflow`
- `show openflow ports [all | <port_list>] {{vlan} <vlan_name>}`
- `configure openflow controller [primary | secondary] [in-band [port <portNumber> | discovery] | out-of-band [active [ipaddress <ipaddress> | hostname <hostName>] {<tcpPort>} | passive <tcpPort>]] {tsl} {vr <vrName>} {rate-limit <rate> {burst-size <burstSize>}}`
- `unconfigure openflow controller [primary | secondary]`
- `show openflow controller {primary | secondary}`
- `show openflow`
- `debug openflow show flows [vendor-table | exos-tree]`

Limitations

- Only supports a single VLAN.
- Supported platforms do not implement both packet and byte counters simultaneously on dynamic ACL entries. Only packet counters are supported.
- IN_PORT and FLOOD forwarding actions are not implemented in hardware, and are instead implemented in the user-space forwarding plane, limiting the throughput that can be sustained for flows using these actions.
- Flows are implemented using ACL hardware. Platform hardware has limitations on the simultaneous combinations of flow match conditions that can be supported. These limitations are described in the platforms' ACL release notes. When receiving a flow match combination that cannot be supported with the platform's ACL hardware, the switch generates an OpenFlow error message to the controller.
- All flow table entries are implemented as wide-key dynamic ACLs, limiting the potential scalability of the flow tables.
- Default emergency flows are not automatically installed, and there is no CLI command to specify them.
- NORMAL forwarding action is not supported.

Supported Platforms

- Summit X440 switches
- Summit X460 switches
- Summit X480 switches
- Summit X670 switches

Generic Routing Encapsulation (GRE) Tunnel Support

This feature allows you to create a Generic Routing Encapsulation (GRE)-based IPv4 tunnel, and route IPv4 traffic over it. This feature supports:

- IPv4-based GRE tunneling support
- Forwarding based on static routes

Limitations

- IPv4 only (both the routed traffic, and tunnel protocol).
- Unicast forwarding only, no Multicast.
- Single IP address can be configured on a GRE tunnel.
- Duplicate Address Detection (DAD) is not supported on GRE tunnels.
- No routing protocol support (RIP, OSPF, etc. etc.), only static routes.
- Maximum of 255 system wide tunnels (this includes any combination of GRE/6in4/6to4).
- On a chassis or SummitStack system, all blades/nodes need to support GRE before the feature can be enabled.
- The GRE capable hardware does not support VRs, so you cannot create tunnels in any other VR than VR-Default. This is the same behavior as for the 6in4/6to4 tunnels.

NOTE

When the hardware matches the tunnel source and destination addresses it does not look at the incoming VR, therefore we do not recommend creating any additional VRs on the switch when using tunnels. If you must, make sure that tunnel traffic on other VRs does not match the tunnels configured on the switch.

Synchronous Ethernet (SyncE) to Derive Timing for Precision Time Protocol (PTP)

The Precise Time Protocol (PTP) synchronizes the network by transferring the master clock information in the form of timestamps in the PTP messages (Sync/FollowUp/DelayReq/DelayResp). In the slave clock, the clock offset is computed through the reception of PTP messages that carry master clock as timestamps.

In practice, a network could employ multiple synchronization methods in the same network. Synchronous Ethernet (SyncE) transfers the frequency of the reference clock through Ethernet's physical layer. The frequency recovered from SyncE is highly accurate when compared to the frequency recovered through PTP messages. However, SyncE does not carry the Time-of-Day (TOD) or the Phase information of the clock as PTP does. Networks that employ SyncE and PTP for synchronization can leverage the accuracy of time transfer through PTP by using SyncE. Such Hybrid networks use SyncE for frequency transfer and PTP for Phase/Time-of-Day transfer.

CLI Commands

- `configure network-clock ptp time-source [network-frequency | ptp-frequency]`
- `show network-clock ptp configuration`

Multi-switch Link Aggregation Groups (MLAG)-Link Aggregation Control Protocol (LACP)

This feature introduces Link Aggregation Control Protocol (LACP) support over Multi-switch Link Aggregation Groups (MLAG) ports with the following options:

- The MLAG peer having the highest IP address for the ISC control VLAN is considered the MLAG LACP master. The switch MAC of the MLAG LACP master is used as the System Identifier by all the MLAG peer switches in the LACPDUs transmitted over the MLAG ports. This is the default option.

- You can configure a common unicast MAC address to be used on all the MLAG peer switches. This MAC address is used as the System Identifier by all the MLAG peer switches in the LACPDUs transmitted over the MLAG ports. This configuration (like any other configuration item is not checkpointed to the MLAG peers) and you have to make sure that the same MAC address is configured on all the MLAG switches. You have to ensure that this address does not conflict with the switch MAC of the server node that teams with the MLAG peer switches.

CLI Commands

```
configure {mlag peer} <peer_name> lacp-mac [auto | <lacp_mac_address>]
```

Multi-session Mirroring

Mirroring is a function on existing Extreme Networks switches which allows copies of packets to be replicated to additional ports without affecting the normal switching functionality. This feature has been revised to support:

- Up to 16 named mirror instances can be created. The system creates a default mirror (“DefaultMirror”) at start of day. This default instance supports legacy CLI operation. You can define up to 15 additional instances.
- You can activate up to four mirror instances, and a mirror with both ingress and egress filters represents two instances. This includes the default instance. If the default instance is not configured, it is not activated.
- Disabling mirroring no longer removes the source filter information. Therefore, you can disable, and then re-enable mirroring if necessary.
- Show commands have been enhanced to allow the following:
  - Legacy show command behaves as before, showing information only about the “default” mirroring instance.
  - Show commands now show a summary list of the configured and enabled mirror instances.
  - Show commands allow you to request detailed information about individual filters.
  - Show commands show detailed information about all configured filters.

Limitations

- SNMP support is limited to what was previously supported in ExtremeXOS.
- No XML support.
- The total number of allowed sources configured in the system is 128. Specifically, only FP filters are a limited resource. Port-based mirroring has no hardware configuration limitations.

ExtremeXOS Network Virtualization (XNV) Dynamic VLAN

This change enhances the ExtremeXOS Network Virtualization (XNV) feature to include dynamic VLAN support:

- Ability to enable/disable the XNV dynamic VLAN feature on a per-port basis.
- Ability to add a VLAN tag and a VR as attributes to both Local and Network Virtual Port Profiles (VPPs).
- Specify the VLAN tag as an attribute to the VM using:
  - For VMs managed through RL, the VM to VLAN tag mapping can be learned from RADIUS or can be specified as part of the mapping entry in the VMMAP file.
  - For VMs managed through CLI, the VM to VLAN tag can be configured through CLI commands.
- If the specified VLAN does not exist, ExtremeXOS dynamically creates the VLAN when the VM is detected and deletes the VLAN when the last VM that uses the VLAN is deleted.
- For VMs sending tagged traffic, if no VLAN configuration exists for the VM, XNV creates the VLAN (assuming the VLAN does not already exist) with the received packet's tag and adds the port to the VLAN as tagged.

Limitations

- As part of VLAN definition, you can only specify the VLAN tag and optionally a VR. ExtremeXOS internally generates names for dynamically created VLANs.
- You can configure a maximum of one tag for the VM as part of either a VM or VPP configuration.
- All restrictions applicable for MVRP-created VLANs are applicable for VLANs created by this feature.
- Dynamically created VLAN are not saved across reboots. However dynamic VLAN information is checkpointed to standby nodes.

- Uplink ports are always added to dynamic VLANs as tagged.
- Since there is time lag between VM detection and programming of the VLAN in hardware, traffic for the first few milliseconds may be flooded on the internal (or default) VLAN or may be dropped.
- This feature is not compatible with NetLogin. This feature cannot be enabled on NetLogin enabled ports.
- Since this feature creates an internal VMAN for VM detection and adds the enabled port as untagged to the internal VMAN, you cannot add the port as untagged to other VMANs.
- Before enabling the dynamic VLAN, you have to add the port to a “default” or “base” VLAN. VMs sending untagged traffic that have no VLAN configuration are classified to this VLAN.

New CLI commands

- `configure vlan dynamic-vlan uplink-ports [ add {ports} <port_list> | delete {ports} [<port_list> | all] ]`
- `show vlan dynamic-vlan`
- `[enable|disable] vm-tracking dynamic-vlan ports <port_list>`
- `configure vm-tracking vpp <vpp_name> vlan-tag <tag> {vr <vr-name>}`
- `unconfigure vm-tracking vpp <vpp_name> vlan-tag`
- `create vm-tracking local-vm mac-address <mac> {name <name> | ip-address <ip_address> | vpp <vpp_name> | vlan-tag <tag> {vr <vr-name>}}`
- `configure vm-tracking local-vm mac-address <mac> [name <name> | ip-address <ipaddress> | vpp <vpp_name> | vlan-tag <tag> {vr <vr-name>}]`
- `unconfigure vm-tracking local-vm mac-address <mac> [name | ip-address | vpp | vlan-tag]`

OpenStack

OpenStack is an open source cloud operating system that manages pools of compute, storage and networking resources. OpenStack has three key projects to offer as-a-service capabilities: compute-as-a-service, storage-as-a-service, and network-as-a-service. This feature introduces a plugin to the network-as-a-service application (Quantum) of OpenStack to provide network-as-a-service capabilities on ExtremeXOS-powered Extreme Network switches. This plugin provides:

- Quantum plugin version 1.1 (Essex) and version 2.0 (Folsom) API support to enable tenants to define network of compute, storage and network services.
- Multitenant isolation with VLAN and VMAN. Multitenant isolation to the compute host via integration with vSwitch from OVS plugin.
- Support for Tenant networks beyond 4K limits using VMAN.
- Support for VM motion across L2 boundaries.
- Support for L3 connectivity and forwarding to and from public/external network via SNAT and floating IPs with Quantum L3 router.
- Support for change management. All changes to tenant networks are logged and tracked for auditing. This is unique to the ExtremeXOS Quantum plugin.
- Transaction Management: Since mapping of virtual to physical networks is a multi-step transaction, each of the transactions is tracked and errors are reported to the north-bound clients. If an error occurs during transaction execution, the entire transaction is rolled back.
- A topology-aware scheduler that chooses compute hosts for new virtual machines (VMs) in close proximity to the other VMs of the tenant. This proximity algorithm minimizes the east-west traffic load, and also reduces switch table sizes. Without this optimization, VMs are placed randomly on any host attached to any switch causing all intermediate switches to learn the VMs, thus causing MAC table exhaustion. The topology aware scheduler also enables tenant networks to scale over the 4K limit by carefully assigning VLAN IDs on a per pod basis. This feature is unique to the Extreme Quantum plugin.

Use Cases

The previous features enable cloud service providers to build the following use cases:

- Cloud-in-a-box: A fully functioning cloud-in-a-box with components: switches, routers, load balancer, firewall, compute and storage. This is economical for enterprises to buy or for cloud resellers to offer as private, hosted cloud service in a data center.
- Private clouds in an enterprise: Enterprises are migrating to cloud services to offer the same services that public clouds offer to their employees. Some of the incentives for this move include: Bring your own device (BYOD), IT central policy enforcements, DevOps, etc.
- Hosted private clouds: As Enterprises try to reduce costs, some enterprises choose to outsource their IT and buy services from cloud service providers.
- Web hosting services: Many small and large web-hosting companies offer low cost web services to consumers. Also, e-commerce companies such as eBay, Zynga, etc. need cloud data centers to scale up and down with demand.

Layer 2 Multi-cast Scaling

This feature provides an option to use the L2 table for IP multicast forwarding database entries to increase scale. It provides an option to use both L2 and IPMC tables for IP multicast forwarding database entries.

Limitations

- The “mixed-mode” configuration option is not allowed on Summit X150, X250e, X350, X450e, X450a, series switches and BlackDiamond 8800 “e2-series” and 8500-G48T-e.
- When the “mixed-mode” configuration option is engaged on BlackDiamond 8800 series switches, newly inserted slots, which do not support “mixed-mode” fail initialization. On SummitStack, this same condition generates the following message every 30 seconds:

  ```
  <HAL.IPv6Mc.Error> Stack slot %d is incompatible with the multicast forwarding lookup configuration. Either remove this node from the stack or change the multicast forwarding lookup configuration.
  ```

- When using the “mac-vlan” configuration option:
  - PIMv4/V6, MVR features cannot be used.
  - IGMPv3 should not be used in conjunction with this mode.
  - Private VLAN multicast should not be used.
  - Issues with IP multicast address to MAC address mapping:

  All IPv4 multicast frames use multicast MAC addresses starting with 01:00:5e:xx:xx:xx. The lower order 23 bits of the IP multicast address are used in the MAC address derivation. As only 23 bits of MAC addresses are available for mapping layer 3 IP multicast addresses to layer 2 MAC addresses, this mapping results in 32:1 address ambiguity. For example, 225.129.1.1 maps to the same MAC address 01:00:5e:01:01:01.

CLI Commands

```
configure forwarding ipmc lookup-key [group-vlan | source-group-vlan | mac-vlan | mixed-mode]
```

In the `show igmp snooping` command, the “Forwarding Lookup-Key” in the output is removed.

255-Character Port Description String

This feature creates a new and separate “description-string” field for each port, which can be up to 255 characters with the same restrictions that exist with the existing “display-string” field. This new field can be set and retrieved via the CLI (`show port` command), SNMP, and XML interfaces.

Limitations

- The following characters cannot be used: ‘ “ ‘, “<”, “>”, “:”, “<space>”, “&”
- SNMP set of the ifAlias element sets both the display-string and the description-string.

CLI Commands

- `[config |unconfig] port <port_list> description-string <string>`
- `config snmp ifmib ifalias size [default | extended]`

Protocol Independent Multi-cast (PIM) Register Filtering

This feature allows to you filter the register message based on the policy file configured on the First-Hop Router (FHR) and/or Rendezvous Point (RP) in the Protocol Independent Multicast-Sparse Mode (PIM-SM) domain. There is a register policy mechanism to filter out specific PIM register messages which have encapsulated specific (S, G) packets. The filtering allows a network administrator to detect/deny malicious multicast packets to flow into a multicast shared tree and then create a service blackout. This is supported for both PIM IPV4 and PIM IPV6 mode.

CLI Commands

```
configure pim {ipv4 | ipv6} register-policy {rp} [<rp_policy_name> |
none]
```

Flow Redirects Increased from 32 to 256

The number of flow redirects is increased from 32 to 256 for both IPv4 and IPv6.

Command to Locate a Switch Using Front Panel LEDs

This new command causes the front panel LEDs to display a unique pattern to allow you to visually locate a switch. The command is not stored and does not survive a reboot.

CLI Commands

- `enable led locator {timeout [<seconds> | none]} {pattern <pattern>} {slot [<slot> | all]`
- `disable led locator {slot [<slot> | all]`

Supported Platforms

- All Summit series switches

New Hardware Supported in ExtremeXOS 15.3

- BlackDiamond X8 10G48T Module
- Summit X440-24t
- Summit X440-48tDC

ExtremeXOS Hardware and Software Compatibility Matrix

The *ExtremeXOS Hardware and Software Compatibility Matrix* provides information about the minimum version of ExtremeXOS software required to support BlackDiamond and Summit switches, as well as SFPs, XENPAKs, XFPs, and other pluggable interfaces.

The latest version of the *ExtremeXOS Hardware and Software Compatibility Matrix* can be found at:

www.extremenetworks.com/documentation/

Upgrading to ExtremeXOS

See “Software Upgrade and Boot Options” in the *ExtremeXOS Concepts Guide* for instructions on upgrading ExtremeXOS software. Following are miscellaneous hitless upgrade notes:

- Beginning with ExtremeXOS 12.1, an ExtremeXOS core image (.xos file) must be downloaded and installed on the alternate (non-active) partition. If you try to download to an active partition, the error message `"Error: Image can only be installed to the non-active partition."` is displayed. An ExtremeXOS modular software package (.xmod file) can still be downloaded and installed on either the active or alternate partition.
- For the BlackDiamond 8800 series switches, a hitless upgrade to ExtremeXOS 15.4 from an earlier release is not supported and should not be attempted. Use the normal software upgrade process for these switches.
- Hitless upgrade from ExtremeXOS 12.0 and earlier to ExtremeXOS 12.1 and later is not supported on the BlackDiamond 12800 switch.
- SummitX software is required for E4G cell site routers.

Downloading Supported MIBs

The Extreme Networks MIBs are located on the eSupport website under Download Software Updates, located at:

https://esupport.extremenetworks.com/

ExtremeXOS Command Line Support

The following is true for all Summit X150 and X350 series switches:

- Summit X150 and X350 series switches do not support L3 functionality; this platform does not support CLI commands for L3 functionality.
- Summit X150 and X350 series switches do not support stacking; all CLI commands for stacking are not supported on this platform.
- Summit X150 and X350 series switches do not support IP forwarding; however, CLI commands that configure IP addresses function in order to access the management functionality of the switch are supported.
- Upgrade or trial licensing is not available on the Summit X150 and X350 series switches.

Tested Third-Party Products

This section lists the third-party products tested for ExtremeXOS 15.2.

Tested RADIUS Servers

The following RADIUS servers are fully tested:

- Microsoft—Internet Authentication Server
- Meetinghouse
- FreeRADIUS

Tested Third-Party Clients

The following third-party clients are fully tested:

- Windows 7
- Windows Vista
- Linux (IPv4 and IPv6)
- Windows XP (IPv4)

PoE Capable VoIP Phones

The following PoE capable VoIP phones are fully tested:

- Avaya 4620
- Avaya 4620SW IP telephone
- Avaya 9620
- Avaya 4602
- Avaya 9630
- Avaya 4621SW
- Avaya 4610
- Avaya 1616
- Avaya one-X
- Cisco 7970
- Cisco 7910
- Cisco 7960
- ShoreTel ShorePhone IP 212k
- ShoreTel ShorePhone IP 560
- ShoreTel ShorePhone IP 560g
- ShoreTel ShorePhone IP 8000
- ShoreTel ShorePhone IP BB 24
- Siemens OptiPoint 410 standard-2
- Siemens OpenStage 20
- Siemens OpenStage 40
- Siemens OpenStage 60
- Siemens OpenStage 80

Extreme Switch Security Assessment

DoS Attack Assessment

Tools used to assess DoS attack vulnerability:

- Network Mapper (NMAP)

ICMP Attack Assessment

Tools used to assess ICMP attack vulnerability:

- SSPing
- Twinge
- Nuke
- WinFreeze

Port Scan Assessment

Tools used to assess port scan assessment:

- Nessus

Service Notifications

To receive proactive service notification about newly released software or technical service communications (for example, field notices, product change notices, etc.), please register at:

www.extremenetworks.com/support/service-notification-form

2 Limits

This chapter summarizes the supported limits in ExtremeXOS 15.3.5-Patch1-3.

Supported Limits

Table 2 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

The term “BlackDiamond 8000 e-series” refers to all BlackDiamond 8500 e-series and 8800 e-series modules.The term “BlackDiamond 8000 series” refers to all BlackDiamond 8500, 8800, and 8900 series modules.

The scaling and performance information shown in Table 2 is provided for the purpose of assisting with network design. It is recommended that network architects and administrators design and manage networks with an appropriate level of network scaling “head room.” The scaling and performance figures provided have been verified using specific network topologies using limited switch configurations. There is no guarantee that the scaling and performance figures shown are applicable to all network topologies and switch configurations and are provided as a realistic estimation only. If you experience scaling and performance characteristics that you feel are sufficiently below what has been documented, contact Extreme Networks technical support for additional assistance.

The route limits shown in Table 2 for IPv4 and IPv6 routing protocols are software limits only. The actual hardware limits may be higher or lower than the software limits, based on platform. The hardware limits for specific platforms are specified as "IPv4/IPv6 routes (LPM entries in hardware)" in the following table.

On products other than the BlackDiamond 8900 xl-series, BlackDiamond X8 series, and Summit X480 series, it is not advised to have greater than 25,000 total IP routes from all routing protocols. 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.

Table 2: Supported Limits

Metric	Product	Limit
AAA (local)—maximum number of admin and local user accounts.	All platforms	16
Access lists (meters)—maximum number of meters.	BlackDiamond 8000 series	
	e-series, group of 24 ports	512
	a-series, group of 24 ports	1,024
	c-series	2,048 ingress, 256 egress
	BlackDiamond 8900 series	
	8900-10G24X-c, group of 12 ports	1,024 ingress, 256 egress
	8900 xl-series, 8900-G96T-c	4,096 ingress, 512 egress
	8900-40G6X-xm	512 ingress 512 egress
	BlackDiamond X8 series	512 ingress, 512 egress
	E4G-200	1,024 ingress 256 egress
	E4G-400	2,048 ingress 256 egress
	Summit X150, X250e, X350, X450e group of 24 ports, Summit X440, X430 per group of 24 ports	512
	Summit X450a, per group of 24 ports	1,024
	Summit X460, E4G-400, per group of 24 ports	2,048 ingress, 256 egress
	Summit X480	4,096 ingress, 512 egress
	Summit 650, group of 12 ports	512 ingress, 256 egress
	Summit X670 with VIM4-40G4x Summit X480 with VIM3-40G4X Summit 650, group of 12 ports with VIM3-40G-4x	512 ingress 512 egress
Access lists (policies)—suggested maximum number of lines in a single policy file.	All platforms	300,000

Table 2: Supported Limits (Continued)

Metric	Product	Limit
Access lists (policies)—maximum number of rules in a single policy file.[a]	BlackDiamond 8000 series	
	a-series, group of 24 ports	2,048
	c-series, group of 24 ports	4,096 ingress, 512 egress
	e-series, group of 24 ports	1,024 ingress
	BlackDiamond 8900	
	8900-10G24X-c modules, group of 12 ports	2,048 ingress, 512 egress
	8900-G96T-c modules, group of 48 ports	8,192 ingress, 1,024 egress
	8900 xl-series	61,440 (up to)
	8900-40G6X-xm	2,048 ingress, 1,024 egress
	BlackDiamond X8 series	2,048 ingress, 1,024 egress
	E4G-200	2,048 ingress, 512 egress
	E4G-400	4,096 ingress, 512 egress
	Summit X150, X250e, X350, X440, X430, X450e group of 24 ports	1,024 ingress
	Summit X450a, group of 24 ports	2,048 ingress
	Summit X460	4,096 ingress, 512 egress
	Summit X480	(up to) 61,440 ingress, 1,024 egress
	Summit X650, group of 12 ports	2,048 ingress, 512 egress
	VIM3-40G4x	2,048 ingress, 1,024 egress
	Summit X670	2,048 ingress
	VIM4-40G4x	1,024 egress
	Summit X480	2048 ingress
	VIM3-40G4X	1024 egress

Table 2: Supported Limits (Continued)

Metric	Product	Limit
Access lists (slices)—number of ACL slices.	BlackDiamond 8000 series	
	a- and c-series, group of 48 ports	16
	e-series, group of 24 ports	8
	BlackDiamond 8900 series	
	8900-10G24X-c modules, group of 12 ports	12 ingress, 4 egress
	8900-G96T-c modules, group of 48 ports	16 ingress, 4 egress
	8900 xl-series	17[b]
	8900-40G6X-xm	10 ingress, 4 egress
	BlackDiamond X8 series	10 ingress, 4 egress
	E4G-200	8 ingress, 4 egress
	E4G-400	16 ingress, 4 egress
	Summit X150, X250e, X350, X450e, group of 48 ports	8 ingress
	Summit X450a, group of 24 ports	16 ingress
	Summit X440	4 ingress
	Summit X460	16 ingress, 4 egress
	Summit X480	17[b] ingress, 4 egress
	Summit X650, group of 12 ports	12 ingress, 4 egress
	VIM3-40G4x	10 ingress, 4 egress
	Summit X670	10 ingress, 4 egress
	VIM4-40G4x	
	Summit X480	
	VIM3-40G4X	10 ingress 4 egress
AVB (audio video bridging)—maximum number of active streams **NOTE:** * It is recommended that you do not use on more than 8 ports on this switch.	Summit X440, X460	1,024
	E4G-400	1,024
	Summit X670	4,096
	Summit X430	100*
BFD sessions—maximum number of BFD sessions	All platforms (default timers)	512
	All platforms (minimal timers)	10[c]
BGP (aggregates)—maximum number of BGP aggregates.	All platforms with Core license or higher	256

Table 2: Supported Limits (Continued)

Metric	Product	Limit
BGP (networks)—maximum number of BGP networks.	All platforms with Core license or higher BlackDiamond X8 series	1,024 1,024
BGP (peers)—maximum number of BGP peers. **NOTE:** * With default keepalive and hold timers.	BlackDiamond X8 series BlackDiamond 8000 series BlackDiamond xl-series Summit X450a, X460, X650, X670 E4G-400, E4G-200 Summit X480	512 512 512 128* 128* 512
BGP (peer groups)—maximum number of BGP peer groups.	BlackDiamond 8900 series BlackDiamond X8 series Summit X480 All platforms (except BlackDiamond X8 series, BlackDiamond 8900 series, and Summit X480) with Core license or higher	128 128 128 64
BGP (policy entries)—maximum number of BGP policy entries per route policy.	All platforms with Core license or higher	256
BGP (policy statements)—maximum number of BGP policy statements per route policy.	All platforms with Core license or higher	1,024
BGP (unicast address-family routes)—maximum number of unicast address-family routes.	BlackDiamond 8000 series BlackDiamond 8900 xl-series BlackDiamond X8 series Summit X450a, X460, X650, X670 Summit X480 E4G-400	25,000 524,256 (up to)[b] 25,000 25,000 524,256 (up to)[b] 25,000
BGP (non-unique routes)—maximum number of non-unique BGP routes.	BlackDiamond 8000 series BlackDiamond 8900 xl-series BlackDiamond X8 series Summit X450a, X460, X650, X670 Summit X480 E4G-400, E4G-200	25,000 1,200,000 25,000 25,000 1,000,000 25,000
BGP ECMP—maximum number of equalcost multipath for BGP and BGPv6.	All platforms except Summit X440	2, 4, or 8

Table 2: Supported Limits (Continued)

Metric	Product	Limit
BGP multi-cast address-family routes —maximum number of multi-cast address-family routes.	BlackDiamond 8000 series BlackDiamond 8900 xl-series BlackDiamond X8 series Summit X450a, X460, X650, X670 Summit X480 E4G-400	25,000 524,256 (up to)[b] 25,000 25,000 524,256 (up to)[b] 25,000
BGPv6 (unicast address-family routes)— maximum number of unicast address family routes.	BlackDiamond 8900 xl-series BlackDiamond 8800 a-, c-series BlackDiamond 8000 e-series BlackDiamond X8 series Summit X450e,X250e Summit X450a, X460, X650 Summit X480 Summit X670 E4G-400	20,000 6,000 240 8,000 240 6,000 20,000 8,000 6,000
BGPv6 (non-unique routes)—maximum number of non-unique BGP routes	BlackDiamond 8900 xl-series BlackDiamond 8800 a-, c-series BlackDiamond 8000 e-series BlackDiamond X8 series Summit X450e,X250e Summit X450a, X460, X650 Summit X480, X670 E4G-400	24,000 18,000 720 24,000 720 18,000 24,000 18,000
BOOTP/DHCP relay—maximum number of BOOTP or DHCP servers per virtual router.	All platforms	4
BOOTP/DHCP relay—maximum number of BOOTP or DHCP servers per VLAN.	All platforms	4
CES TDM pseudo wires—maximum number of CES TDM pseudo wires per switch.	E4G-200 and E4G-400	256
Connectivity fault management (CFM)—maximum number or CFM domains.	All platforms	8
CFM—maximum number of CFM associations.	All platforms	256
CFM—maximum number of CFM up end points.	BlackDiamond 8000 series BlackDiamond X8 series Summit series	32 32 32

Table 2: Supported Limits (Continued)

Metric	Product	Limit
CFM—maximum number of CFM down end points.	BlackDiamond 8000 series	32
	BlackDiamond X8 series	32
	Summit series X460, E4G-200, E4G-400 (non-load shared ports)	256
	Summit series X460, E4G-200, E4G-400 (load shared ports)	32
	Summit series	32
	All other platforms	32
CFM—maximum number of CFM remote end points per up/down end point.	All platforms	2,000
CFM—maximum number of dot1ag ports.	All platforms	128
CFM—maximum number of CFM segments.	All platforms	1,000
CLEAR-Flow—total number of rules supported. The ACL rules plus CLEAR-Flow rules must be less than the total number of supported ACLs.	BlackDiamond 8800 c-series	4,096
	BlackDiamond 8900 series	4,096
	BlackDiamond X8 series	4,096
	Summit X440	1,024
	Summit X450a, X650, X670	2,048
	Summit X480	4,096
Data Center Bridging eXchange (DCBX) protocol Type Length Value (TLVs)—maximum number of DCBX application TLVs.	All platforms	8
Dynamic ACLs—maximum number of ACLs processed per second. **NOTE:** Limits are load dependent.	BlackDiamond 8800 with c-series MSM and I/O modules	8
	BlackDiamond 8900 series	8
	BlackDiamond X8 series	8
	Summit X450a, X480, X650, X670	
	with 50 DACLs	10
	with 500 DACLs	5
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 8000 series	64
	BlackDiamond X8 series	64
	Summit series (except X430), E4G-200, E4G-400	32
	Summit X430	8
EAPSv1 protected VLANs—maximum number of protected VLANs.	BlackDiamond 8000 series	2,000
	BlackDiamond X8 series	4,000
	Summit series, E4G-200, E4G-400	1,000

Table 2: Supported Limits (Continued)

Metric	Product	Limit
EAPSv2 protected VLANs—maximum number of protected VLANs.	BlackDiamond 8000 series BlackDiamond X8 series Summit series, E4G-200, E4G-400	2,000 4,000 500
ELSM (vlan-ports)—maximum number of VLAN ports.	BlackDiamond 8000 series BlackDiamond X8 series Summit series, E4G-200, E4G-400	5,000 5,000 5,000
ERPS domains—maximum number of ERPS domains without CFM configured	BlackDiamond 8806 series BlackDiamond X8 series Summit series (except X430), E4G-200, E4G-400 Summit X430	32 32 32 4
ERPS domains—maximum number of ERPS domains with CFM configured.	BlackDiamond 8806 series BlackDiamond X8 series Summit series non-CSR platforms Summit X460 E4G-200, E4G-400	16 16 16 32 32
ERPSv1 protected VLANs—maximum number of protected VLANs.	BlackDiamond 8806 series BlackDiamond X8 series Summit series, E4G-200, E4G-400	2,000 2,000 1,000
ERPSv2 protected VLANs—maximum number of protected VLANs	BlackDiamond 8806 series BlackDiamond X8 series Summit series, E4G-200, E4G-400	2,000 2,000 500
ESRP groups—maximum number of ESRP groups.	All platforms	7
ESRP domains—maximum number of ESRP domains.	BlackDiamond 8000 series BlackDiamond X8 series BlackDiamond 8900 series Summit series	64 64 128 64
ESRP VLANs—maximum number of ESRP VLANs.	BlackDiamond 8000 series BlackDiamond X8 and 8900 series Summit series	1,000 2,048 1,000
ESRP (maximum ping tracks)—maximum number of ping 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

Table 2: Supported Limits (Continued)

Metric	Product	Limit
Forwarding rate—maximum L2/ L3 software forwarding rate.	BlackDiamond 8000 series	10,000 pps
	BlackDiamond X8 series	20,000 pps
	Summit series	10,000 pps
FDB (blackhole entries)— maximum number of unicast blackhole FDB entries.	BlackDiamond 8800 a-series	16,000
	BlackDiamond 8800 c-series	32,000
	BlackDiamond 8000 e-series	8,000
	BlackDiamond 8900 series	
	8900 c-series 8900 xl-series	32,000 524,288 (up to)[b]
	8900-40G6X-xm	128,000
	BlackDiamond X8 series	128,000
	E4G-200, E4G-400	32,000
	Summit X150, X250e, X350, X450e	8,000
	Summit X440, X450a, X430	16,000
	Summit X480	524,288 (up to)[b]
	Summit X460	32,000
	Summit X650	
	VIM3-40G4x	32,000
	Summit X670	
	VIM4-40G4x	128,000
FDB (blackhole entries)— maximum number of multi-cast blackhole FDB entries.	BlackDiamond 8000 series	1,024
	BlackDiamond X8 series	1,024
	All Summit series switches	1,024

Table 2: Supported Limits (Continued)

Metric	Product	Limit
FDB (maximum L2 entries)—maximum number of MAC addresses.	BlackDiamond 8800 a-series	16,384[d]
	BlackDiamond 8000 c-series	32,768[d]
	BlackDiamond 8000 e-series	8,192[d]
	BlackDiamond 8000 (system), except 8900 xl-series	128,000[d]
	BlackDiamond 8900 xl-series	524,488 (up to)[b]
	BlackDiamond X8 series	128,000[d]
	E4G-200, E4G-400	32,000[d]
	Summit X150, X350, X250e, X450e	8,192[d]
	Summit X440, X430	16,000[d]
	Summit X450a	16,384[d]
	Summit X480	524,488 (up to)[b]
	Summit X480 VIM3-40G4X	128,000[d]
	Summit X460, 650	32,768[d]
	SummitStack (except X480)	128,000[d]
	Summit X670	128,000[d]
FDB (Maximum L2 entries)—maximum number of multi-cast FDB entries.	BlackDiamond X8 BlackDiamond 8800 All Summit series switches	1,024
FIP Snooping VLANs	BlackDiamond X8	768
	BlackDiamond 8800 (8900-40G6X-c only)	
	Summit X670	
	Summit X650 series	
FIP Snooping Virtual Links (FPMA mode) per port group	BlackDiamond X8	1,908
	BlackDiamond 8800 (8900-40G6X-c only)	
	Summit X670	
	Summit X650 series	
FIP Snooping FCFs (with perimeter port) per port group	BlackDiamond X8	238
	BlackDiamond 8800 (8900-40G6X-c only)	
	Summit X670	
	Summit X650 series	

Table 2: Supported Limits (Continued)

Metric	Product	Limit
FIP Snooping FCFs (with Enode-to-FCF port)	BlackDiamond X8	212
	BlackDiamond 8800 (8900-40G6X-c only)	
	Summit X670	
	Summit X650 series	
Identity management— maximum number of Blacklist entries.	All platforms	512
Identity management— maximum number of Whitelist entries.	All platforms	512
Identity management— maximum number of roles that can be created.	All platforms	64
Identity management— maximum role hierarchy depth allowed.	All platforms	5
Identity management— maximum number of attribute value pairs in a role match criteria.	All platforms	16
Identity management— maximum of child roles for a role.	All platforms	8
Identity management— maximum number of policies/ dynamic ACLs that can be configured per role.	All platforms	8
Identity management— maximum number of LDAP servers that can be configured.	All platforms	8
Identity management— maximum number of Kerberos servers that can be configured.	All platforms	20
Identity management— maximum database memory-size.	All platforms	64–49, 152
Identity management— recommended number of identities per switch. **NOTE:** Number of identities per switch is for a default identity management database size (512 Kbytes) across all platforms.	All platforms	100

Table 2: Supported Limits (Continued)

Metric	Product	Limit
Identity management— recommended number of ACL entries per identity. **NOTE:** Number of ACLs per identity based on system ACL limitation.	All platforms	20
Identity management— maximum number of dynamic ACL entries configured as an individual dynamic rule, or as an ACL entry in a policy file.	All platforms (except Summit X430) Summit X430	500 256
IGMP sender—maximum number of IGMP senders per switch (IP multi-cast compression disabled).[i] **NOTE:** Assumes source-group-vlan mode.	BlackDiamond 8800 a-series BlackDiamond 8800 c-series BlackDiamond 8000 e-series BlackDiamond 8900-10G24X-c modules BlackDiamond 8900-G96T-c modules BlackDiamond 8900-40G6X-xm BlackDiamond 8900 xl-series BlackDiamond X8 series E4G-200, E4G-400 Summit X150, X250e, X350, X450e Summit X440 Summit X450a Summit X480 Summit X460 Summit X650 VIM3-40G4x Summit X670 VIM4-40G4x	1,024 2,048[e] 500[f] 2,048[e] 4,096[e] 3,000[f] 4,096[e] 4,096[g] 2,048 500[f] 64 1,024 4,096 2,048 2,048 3,000[f] 3,000[f]

Table 2: Supported Limits (Continued)

Metric	Product	Limit
IGMP sender—maximum number of IGMP senders per switch (IP multi-cast compression enabled).[i] **NOTE:** Assumes source-group-vlan mode. For additional limits, see: • Layer-2 IPMC forwarding caches—(IGMP/MLD/PIM snooping) in mac-vlan mode. on page 72 • Layer-2 IPMC forwarding caches— (IGMP/MLD/PIM snooping) in mixed-mode. on page 73	BlackDiamond 8800 a-series BlackDiamond 8800 c-series BlackDiamond 8000 e-series BlackDiamond 8900 c-series BlackDiamond 8900 xl-series BlackDiamond 8900-40G6X-xm BlackDiamond X8 series E4G-200 E4G-400 Summit X150, X250e, X350, X450e Summit X440 Summit X450a Summit X460 Summit X480 Summit X650 VIM3-40G4x Summit X670 VIM4-40G4x	2,000[f] 6,000[f] 500[f] 6,000[f] 12,000[b] 3,000[f] 6,000[f] [g] 3,000[f] 6,000[f] 500[f] 192[f] 2,000[f] 6,000[f] 12,000[b] 6,000[f] 3,000[f] 3,000[f]
IGMP snooping per VLAN filters—maximum number of VLANs supported in per-VLAN IGMP snooping mode.	BlackDiamond 8800 a-series BlackDiamond 8800 c-series BlackDiamond 8000 e-series BlackDiamond 8900 c-series BlackDiamond 8900 xl-series BlackDiamond 8900-40G6X-xm BlackDiamond X8 series E4G-200, E4G-400 Summit X150, X250e, X350, X440 X450e Summit X450a, X460, X650, X670 Summit X480	1,000 2,000 448 1,000 4,000 1,000 1,000 1,000 448 1,000 4,000
IGMPv1/v2 SSM-map entries—maximum number of IGMPv1/v2 SSM mapping entries.	All platforms	500
IGMPv1/v2 SSM-MAP entries—maximum number of sources per group in IGMPv1/v2 SSM mapping entries.	All platforms	50

Table 2: Supported Limits (Continued)

Metric	Product	Limit
IGMPv2 subscriber—maximum number of IGMPv2 subscribers per port.[j]	BlackDiamond 8800 c-series	2,000
	BlackDiamond 8900 c-series	2,000
	BlackDiamond X8 series	2,000
	Summit series (except Summit X460, X480, X650, and X670)	1,000
	Summit X460, X480, X650, X670, E4G-400	2,000
IGMPv2 subscriber—maximum number of IGMPv2 subscribers per switch.[j]	BlackDiamond 8800 c-series	20,000
	BlackDiamond 8900 c-series	20,000
	BlackDiamond X8 series	20,000
	Summit series (except Summit X480, X650, and X670)	10,000
	Summit X460, X480, X650, X670, E4G-400	20,000
IGMPv3 maximum source per group—maximum number of source addresses per group.	All platforms	250
IGMPv3 subscriber—maximum number of IGMPv3 subscribers per port.[j]	BlackDiamond 8800 a-, e-series	1,000
	BlackDiamond 8800 c-series	2,000
	BlackDiamond 8900 series	5,000
	BlackDiamond X8 series	3,000
	Summit series (except Summit X460)	1,000
	Summit X460, E4G-400	2,000
IGMPv3 subscriber—maximum number of IGMPv3 subscribers per switch.[j]	BlackDiamond 8800 a-, e-series	10,000
	BlackDiamond 8800 c-series	20,000
	BlackDiamond 8900 series	30,000
	BlackDiamond X8 series	30,000
	Summit series (except Summit X460)	10,000
	Summit X460, E4G-400	20,000
IP ARP entries in software—maximum number of IP ARP entries in software. **NOTE:** May be limited by hardware capacity of FDB (maximum L2 entries).	All platforms	20,480

Table 2: Supported Limits (Continued)

Metric	Product	Limit
IP ARP entries in software with distributed mode on—maximum number of IP ARP entries in software with distributed mode on.	BlackDiamond 8000 series with 8900-MSM128 or MSM-48c, and only 8900 xl-series I/O modules	260,000
	BlackDiamond 8000 series with any I/O modules that are not 8900 xl-series	100,000
	BlackDiamond X8 series	28,000
	All other platforms	N/A
IPv4 ARP entries in hardware with distributed mode on—maximum number of IP ARP entries in hardware with distributed mode on	Per BlackDiamond 8900-10G8X-xl, up to 260,000 per system	32,500[b]
	Per BlackDiamond 8900-G48X-xl or 8900-G48T-xl, up to 130,000 per system	16,250[b]
	Per BlackDiamond 8000 c-series, up to 18,000 per system	8,000
	BlackDiamond 8900-40G6X-xm, up to 22,000 per system	8,000
	BlackDiamond X8 series, up to 28,000 per system	12,000
	All other platforms	N/A
IPv4 ARP entries in hardware with minimum LPM routes—maximum recommended number of IPv4 ARP entries in hardware, with minimum LPM routes present. For BlackDiamond 8800, BlackDiamond X8, E4G, and Summit series switches, assumes number of IP route reserved entries is 100 or less.	BlackDiamond 8800 a-, c-, xm-series	8,000
	BlackDiamond 8000 e-series	1,000[f]
	BlackDiamond 8900 xl-series	16,000
	BlackDiamond X8 series	16,000
	E4G-200	8,000
	E4G-400	16,000
	Summit X440	412
	Summit X250e, X450e	1,000[f]
	Summit X450a, X650, X670	8,000
	Summit X460, X480	16,000
IPv4 ARP entries in hardware with maximum LPM routes—maximum recommended number of IPv4 ARP entries in hardware, with maximum LPM routes present. For BlackDiamond 8800, BlackDiamond X8, E4G, and Summit series, assumes number of IP route reserved entries is "maximum."	BlackDiamond 8800 a-series	2,000[f]
	BlackDiamond 8800 c-, xm-series	6,000[f]
	BlackDiamond 8000 e-series	500[f]
	BlackDiamond 8900 xl-series	12,000[f]
	BlackDiamond X8 series	12,000[f]
	E4G-200	6,000[f]
	E4G-400	12,000[f]
	Summit X440	380
	Summit X250e, X450e	500[f]
	Summit X450a	2,000[f]
	Summit X460, X480	12,000[f]
	Summit X650, X670	6,000[f]

Table 2: Supported Limits (Continued)

Metric	Product	Limit
IPv4 remote hosts in hardware with zero LPM routes— maximum recommended number of IPv4 remote hosts (hosts reachable through a gateway) in hardware when LPM routing is not used. For BlackDiamond 8800, BlackDiamond X8, E4G, and Summit series, assumes number of IP route reserved entries is 0, and number of IPv4 ARP entries present is 100 or less.	BlackDiamond 8800 a-series	14,000[f]
	BlackDiamond 8800 c-series	18,000[f]
	BlackDiamond 8000 e-series	1,000[f]
	BlackDiamond 8900 xl-series	40,000[b]
	BlackDiamond 8900-40G6X-xm	22,000[f]
	BlackDiamond X8 series	28,000[f]
	E4G-200	18,000[f]
	E4G-400	20,000[f]
	Summit X440	448
	Summit X250e, X450e	1,000[f]
	Summit X450a	14,000[f]
	Summit X460	20,000[f]
	Summit X480	40,000[b]
	Summit X650	18,000[f]
	Summit X670	22,000[f]
IPv4 routes—maximum number of IPv4 routes in software (combination of unicast and multi-cast routes).	BlackDiamond 8900 xl-series with 8900-MSM128 or MSM-48c	524,256 (up to)[b]
	All other BlackDiamond 8000 series hardware	25,000
	BlackDiamond X8 series	25,000
	Summit X440	256
	Summit X250e, X450a, X450e, X460, X650, X670, E4G-400, E4G-200	
	SummitStack or standalone	25,000
	Summit X480	
	SummitStack or standalone	524,256 (up to)[b]
IPv4 routes (LPM entries in hardware)— number of IPv4 routes in hardware.	BlackDiamond 8800 a-, c-series	12,000
	BlackDiamond 8000 e-series	480
	BlackDiamond 8900 xl-series	524,256 (up to)[bh]
	BlackDiamond 8900-40G6X-xm	16,000[e]
	BlackDiamond X8 series	16,000[e]
	E4G-200, E4G-400	12,000
	Summit X440	32
	Summit X250e, X450e	480
	Summit X450a, X460, X650	12,000
	Summit X480	524,256 (up to)[bh]
	Summit X670	16,000[h]

Table 2: Supported Limits (Continued)

Metric	Product	Limit
IPv6 addresses on an interface—maximum number of IPv6 addresses on an interface.	All platforms	255
IPv6 addresses on a switch—maximum number of IPv6 addresses on a switch	BlackDiamond 8000 series BlackDiamond X8 series E4G-200, E4G-400 Summit X440 Summit X460, X480, X650, X670	512 512 512 254 512
IPv6 host entries in hardware—maximum number of IPv6 neighbor entries in hardware.	BlackDiamond 8800 a-series BlackDiamond 8800 c-, xm-series BlackDiamond 8000 e-series BlackDiamond 8900-10G24X-c modules BlackDiamond 8900-G96T-c modules BlackDiamond 8900 xl-series BlackDiamond X8 series E4G-200 E4G-400 Summit X440 Summit X250e, X450e Summit X450a Summit X460, X670 Summit X650 Summit X480	1,000[f] 3,000[f] 250[f] 2,000[f] 4,000[f] 8,192 (up to)[b] 3,000[f] 2,000[f] 3,000[f] 192 250[f] 1,000[f] 3,000[f] 2,000[f] 8,192 (up to)[b]
IPv6 route sharing in hardware—route mask lengths for which ECMP is supported in hardware.	Summit X460, X480, X670, X670V-48t E4G-200, E4G-400 BlackDiamond 8800 (all I/O modules, except G48Te2), BlackDiamond X8 10G and 40G Summit X460-G2, X670-G2, X770 BlackDiamond 8800 G48Te2, BlackDiamond X8 100G Summit X440	0–128 0–128 0–128 0–64 (> 64 single path only) 0–64 (> 64 single path only) Single path only

Table 2: Supported Limits (Continued)

Metric	Product	Limit
IPv6 routes (LPM entries in hardware)—maximum number of IPv6 routes in hardware.	BlackDiamond 8800 a-, c-series	6,000
	BlackDiamond 8000 e-series	240
	BlackDiamond 8900 xm-series	8,000
	BlackDiamond 8900 xl-series	245,760 (up to)[b]
	BlackDiamond X8 series	8,000
	E4G-200, E4G-400	6,000
	Summit X440	16
	Summit X250e, X450e	240
	Summit X450a, X460, X650	6,000
	Summit X670	8,000
	Summit X480	245,760 (up to)[b]
IPv6 routes with a mask greater than 64 bits in hardware—maximum number of such IPv6 LPM routes in hardware.	BlackDiamond 8000 a-, c-, e-, xm-series	256
	BlackDiamond 8000 xl-series	245,760 (up to)[b]
	BlackDiamond X8 series	256
	E4G-200, E4G-400	256
	Summit X250e, X440, X450e, X450a, X460, X650, X670	256
	Summit X480	245,760 (up to)[b]
IPv6 routes in software—maximum number of IPv6 routes in software.	BlackDiamond 8900 xl-series with 8900-MSM128 or MSM-48c	245,760 (up to)[b]
	All other BlackDiamond 8000 series hardware	25,000
	BlackDiamond X8 series	25,000
	Summit X250e, X450a, X450e, X460, X650, X670, E4G-200, E4G-400, SummitStack, or standalone	25,000
	Summit X440	256
	Summit X480, SummitStack, or standalone	245,760 (up to)[b]
IP router interfaces—maximum number of VLANs performing IP routing–excludes sub VLANs (IPv4 and IPv6 interfaces).	BlackDiamond X8 series	512
	All BlackDiamond 8000 series and Summit family switches with Edge license or higher	512
IP multi-cast static routes—maximum number of permanent multi-cast IP routes.	All platforms	1,024
IP unicast static routes—maximum number of permanent IP unicast routes.	All platforms	1,024

Table 2: Supported Limits (Continued)

Metric	Product	Limit
IP route sharing (maximum gateways)—configurable maximum number of configurable gateways used by equal cost multipath OSPF, BGP, IS-IS, or static routes. Routing protocols OSPF, BGP, and IS-IS are limited to 8 ECMP gateways per destination.	All platforms	2, 4, 8, 16, or 32
IP route sharing (total destinations)—maximum number of unique destinations used by multipath OSPF, OSPFv3, BGP, IS-IS, or static routes. **NOTE:** For platforms with limit of 524,256, the total number of "destination+gateway" pairs is limited to 1,048,512. For example, if the number of unique destinations is 524,256, only 2 gateways per destination is supported. For other platforms, each limit is based on up to 8 gateways per destination for routing protocols, or up to 32 gateways per destination for static routes.	BlackDiamond 8800 a-series, c-series BlackDiamond 8000 e-series BlackDiamond 8900 xl-series BlackDiamond 8900-40G6X-xm BlackDiamond X8 series Summit X250e, X450e Summit X450a, X460, X650, E4G-200, E4G-400 Summit X480 Summit X670 E4G-200, E4G-400	12,256 480 524,256 (up to)[b] 16,352 16,000 480 12.256 524,256 (up to)[b] 16,352 12,256

Table 2: Supported Limits (Continued)

Metric	Product	Limit
IP route sharing (total combinations of gateway sets)—maximum number of combinations of sets of adjacent gateways used by multipath OSPF, BGP, IS-IS, or static routes.	BlackDiamond 8800 a-, c-, xl-, and xm-series	
	default maximum gateways of 4	510
	if maximum gateways is 2	1,022
	if maximum gateways is 8	254
	if maximum gateways is 16	126
	if maximum gateways is 32	62
	BlackDiamond 8000 e-series	
	default maximum gateways of 4	30
	if maximum gateways is 2	62
	if maximum gateways is 8	14
	if maximum gateways is 16	6
	if maximum gateways is 32	2
	BlackDiamond X8 series	
	default maximum gateways of 4	510
	if maximum gateways is 2	1,022
	if maximum gateways is 8	254
	if maximum gateways is 16	126
	if maximum gateways is 32	62
	Summit X460, X480, X650, X670, E4G-200, E4G-400	
	default maximum gateways of 4	510
	if maximum gateways is 2	1,022
	if maximum gateways is 8	254
	if maximum gateways is 16	126
	if maximum gateways is 32	62
IP multinetting (secondary IP addresses)—maximum number of secondary IP addresses per VLAN.	All platforms	64
IS-IS adjacencies—maximum number of supported IS-IS adjacencies.	BlackDiamond 8000 series	128
	BlackDiamond X8 series	128
	BlackDiamond 8900 xl-series	255
	Summit X450a, X460, X480, X650, X670, E4G-400	128
	E4G-200	256
IS-IS ECMP—maximum number of equal cost multipath for IS-IS.	All platforms, except Summit X440	2, 4, or 8
IS-IS interfaces—maximum number of interfaces that can support IS-IS.	All platforms	255
IS-IS routers in an area—recommended maximum number of IS-IS routers in an area.	Summit X480	128
	All other platforms	256

Table 2: Supported Limits (Continued)

Metric	Product	Limit
IS-IS route origination—recommended maximum number of routes that can be originated by an IS-IS node.	BlackDiamond 8000 series BlackDiamond X8 series BlackDiamond 8900 xl-series Summit X450a Summit X480 Summit X460, X650, X670, E4G-400 E4G-200	20,000 20,000 30,000 5,000 30,000 20,000 25,000
IS-IS IPv4 L1 routes in an L1 router—recommended maximum number of IS-IS Level 1 routes in a Level 1 IS-IS router.	BlackDiamond 8000 series BlackDiamond X8 series BlackDiamond 8900 xl-series Summit X450a Summit X480 Summit X460, X650, X670, E4G-400	25,000 25,000 120,000 5,000 50,000 25,000
IS-IS IPv4 L2 routes—recommended maximum number of IS-IS Level 2 routes.	BlackDiamond 8000 series BlackDiamond X8 series BlackDiamond 8900 xl-series Summit X450a Summit X480 Summit X460, X650, X670, E4G-400	25,000 25,000 120,000 5,000 50,000 25,000
IS-IS IPv4 L1 routes in an L1/L2 router—recommended maximum number of IS-IS Level 1 routes in an L1/L2 IS-IS router.	BlackDiamond 8000 series BlackDiamond X8 series BlackDiamond 8900 xl-series Summit X450a Summit X460, X480, X650, X670, E4G-400	20,000 20,000 20,000 20,000 20,000
IS-IS IPv6 L1 routes in an L1 router—recommended maximum number of IS-IS Level 1 routes in a Level 1 IS-IS router.	BlackDiamond 8000 series BlackDiamond X8 series BlackDiamond 8900 xl-series Summit X450a Summit X480 Summit X460, X650, X670, E4G-400	10,000 10,000 40,000 5,000 25,000 10,000
IS-IS IPv6 L2 routes—recommended maximum number of IS-IS Level 2 routes.	BlackDiamond 8000 series BlackDiamond X8 series BlackDiamond 8900 xl-series Summit X450a Summit X480 Summit X460, X650, X670, E4G-400	10,000 10,000 40,000 5,000 25,000 10,000

Table 2: Supported Limits (Continued)

Metric	Product	Limit
IS-IS IPv6 L1 routes in an L1/L2 router—recommended maximum number of IS-IS Level 1 routes in a L1/l2 router.	BlackDiamond 8000 series BlackDiamond X8 series BlackDiamond 8900 xl-series Summit X450a Summit X480 Summit X460, X650, X670, E4G-400	10,000 10,000 15,000 3,000 15,000 10,000
IS-IS IPv4/IPv6 L1 routes in an L1 router—recommended maximum number of IS-IS Level 1 routes in a Level 1 IS-IS router. The numbers documented are based on 50% IPv4 routes and 50% IPv6 routes.	BlackDiamond 8000 series BlackDiamond X8 series BlackDiamond 8900 xl-series Summit X450a Summit X480 Summit X460, X650, X670, E4G-400	20,000 20,000 60,000 5,000 40,000 20,000
IS-IS IPv4/IPv6 L2 routes in an L2 router—recommended maximum number of IS-IS Level 2 routes in a Level 2 IS-IS router. The numbers documented are based on 50% IPv4 routes and 50% IPv6 routes.	BlackDiamond 8000 series BlackDiamond X8 series BlackDiamond 8900 xl-series Summit X450a Summit X480 Summit X460, X650, X670, E4G-400	20,000 20,000 60,000 5,000 40,000 20,000
IS-IS IPv4/IPv6 L1 routes in an L1/L2 router—recommended maximum number of IS-IS Level 1 routes in a Level 1/ Level2 IS-IS router. The numbers documented are based on 50% IPv4 routes and 50% IPv6 routes.	BlackDiamond 8000 series BlackDiamond X8 series BlackDiamond 8900 xl-series Summit X450a Summit X460, X480, X650, X670, E4G-400	20,000 20,000 20,000 3,000 20,000
Jumbo frames—maximum size supported for jumbo frames, including the CRC.	All platforms	9,216
Layer-2 IPMC forwarding caches—(IGMP/MLD/PIM snooping) in mac-vlan mode. **NOTE:** IPv6 and IPv4 L2 IPMC scaling is the same for this mode.	BlackDiamond 8800 e-series switches BlackDiamond 8800 c- and xl-series switches BlackDiamond 8800 xm-series switches BlackDiamond X8 series switches E4G-200 and E4G-400 cell site routers, Summit X460, X480, X650 Summit X670 Summit X150 ,X250, X350, X450e Summit X450a, X440	2,000 8,000 15,000 15,000 8,000 15,000 2,000 4,000

Table 2: Supported Limits (Continued)

Metric	Product	Limit
Layer-2 IPMC forwarding caches—(IGMP/MLD/PIM snooping) in mixed-mode. **NOTE:** IPv6 and IPv4 L2 IPMC scaling is the same for this mode.	BlackDiamond 8800 e-series switches	N/A
	BlackDiamond 8800 xl- and c-series switches	8,000
	BlackDiamond 8800 xm-series switches	15,000
	BlackDiamond X8, Summit X670	15,000
	E4G-200 and E4G-400 cell site routers, Summit X460, X480, X650	8,000
	Summit X150, X250, X350, X450, X450a, X450e	N/A
	Summit X440	4,000
Layer-3 IPMC forwarding caches—(PIM, MVR, PVLAN) in mixed-mode.[f] **NOTE:** IPv6 L3 IPMC scaling is 50% of these limits in this mode.	BlackDiamond 8800 e-series switches	N/A
	BlackDiamond 8800 xl- and c-series switches	6,000
	BlackDiamond 8800 xm-series switches	3,000
	BlackDiamond X8 series switches	6,000
	E4G-200 cell site routers, Summit X670	3,000
	E4G-400 cell site routers, Summit X460, X480, X650	6,000
	Summit X150, X250, X350, X450e, X450a	N/A
	Summit X440	192

Table 2: Supported Limits (Continued)

Metric	Product	Limit
Load sharing—maximum number of loadsharing groups. **NOTE:** The actual number of load-sharing groups that can be configured is limited by the number of physical ports present in the switch or SummitStack.	BlackDiamond 8000 series without 8900-40G6X-xm	
	With distributed IP ARP mode off (default)	128
	With distributed IP ARP mode on	64
	BlackDiamond 8000 series with 8900-40G6X-xm using address-based custom algorithm	
	With distributed IP ARP mode off (default)	128
	With distributed IP ARP mode on	64
	BlackDiamond 8000 series with 8900-40G6X-xm with L2, L3 or L3_L4 algorithm configured for any group	
	With distributed IP ARP mode off (default)	127
	With distributed IP ARP mode on	63
	SummitStack with X670 with L2, L3 or L3_L4 algorithm configured for any group	127
	All other SummitStack configurations and Summit series switches	128
	BlackDiamond X8 series using address-based custom algorithm	
	With distributed IP ARP mode off (default)	384
	With distributed IP ARP mode on	384
	BlackDiamond X8 series with L2, L3 or L3_L4 algorithm configured for any group	
	With distributed IP ARP mode off (default)	127
	With distributed IP ARP mode on	63
Load sharing—maximum number of ports per load-sharing group.	BlackDiamond X8 series	64
	Summit X670 (non-stacked)	32
	SummitStack of all X670s	64
	All other Summit series, SummitStacks, and BlackDiamond 8000 series switches	8
Logged messages—maximum number of messages logged locally on the system.	All platforms	20,000
MAC address learning rate—hardware learning rate	E4G-200	22 msec
MAC-based security—maximum number of MAC-based security policies.	All platforms	1,024

Table 2: Supported Limits (Continued)

Metric	Product	Limit
Mirroring (filters)—maximum number of mirroring filters. **NOTE:** This is the number of filters across all the active mirroring instances.	BlackDiamond 8000 series BlackDiamond X8 series Summit series	128 128 128
Mirroring (monitor port)—maximum number of monitor ports.	All platforms	1
Mirroring, one-to-many (filters)—maximum number of one-to-many mirroring filters. **NOTE:** This is the no. of filters across all the active mirroring instances	BlackDiamond 8000 series BlackDiamond X8 series Summit series	128 128 128
Mirroring, one-to-many (monitor port)—maximum number of one-to-many monitor ports.	All platforms	16
Maximum mirroring instances **NOTE:** Only two or four mirroring instance will be active at a time depending on the mirroring filter added to it. There are four hardware resource slots. Each single instance uses one such slot, while each ingress plus egress instance uses two slots. So this allows the you to use a total of four slots, while there are no more then two egress instances. The maximum possible combination for mirroring instances: 1 4 ingress 2 3 ingress + 1 egress 3 2 ingress + 2 egress 4 2 (ingress + egress) 5 1 (ingress + egress) + 2 ingress 6 1 (ingress + egress) + 1 egress + 1 ingress	All platforms	16 (including default mirroring instance)
MLAG ports—maximum number of MLAG ports allowed.	BlackDiamond 8800 series BlackDiamond X8 series Summit series	768 768 768

Table 2: Supported Limits (Continued)

Metric	Product	Limit
MLAG peers—maximum number of MLAG peers allowed.	BlackDiamond 8800 series BlackDiamond X8 series Summit series	1 1 1
MPLS LDP enabled interfaces—maximum number of MPLS LDP configured interfaces per switch.	Summit X460 Summit X480 Summit X480-40G VIM Summit X670 Summit X670V-48t BlackDiamond 8900 xl-series BlackDiamond 8900-40G6x-xm BlackDiamond X8 series E4G-200 E4G-400	32 64 64 32 64 64 64 64 32 32
MPLS LDP fast reroute—MPLS LDP fast reroute (FRR) switching time.	E4G-200	50 msec
MPLS LDP peers—maximum number of MPLS LDP peers per switch.	Summit X460 Summit X480, Summit X480-40G VIM Summit X670 Summit X670V-48t BlackDiamond 8900 xl-series BlackDiamond 8900-40G6x-xm BlackDiamond X8 series E4G-400, E4G-200	32 64 32 64 64 64 64 32
MPLS LDP adjacencies—maximum number of MPLS LDP adjacencies per switch.	BlackDiamond 8900 xl-series BlackDiamond 8900-40G6x-xm BlackDiamond X8 series E4G-200, E4G-400 Summit X460, X480, X670 Summit X670V-48t, Summit X480-40G VIM	50 64 50 50 50 64
MPLS LDP ingress LSPs—maximum number of MPLS LSPs that can originate from a switch.	BlackDiamond 8900 xl-series BlackDiamond 8900-40G6X-xm BlackDiamond X8 series E4G-200 E4G-400 Summit X460, X480 Summit X670, Summit X670V-48t, Summit X480-40G VIM	4,000 2,048 2,048 2,048 4,000 4,000 2,048

Table 2: Supported Limits (Continued)

Metric	Product	Limit
MPLS LDP Sessions—maximum number of MPLS LDP sessions.	E4G-200	32
MPLS LDP transit LSPs—maximum number of MPLS transit LSPs per switch.	BlackDiamond 8900 xl-series BlackDiamond 8900-40G6X-xm BlackDiamond X8 series E4G-200 E4G-400 Summit X460, Summit X480 Summit X670 Summit X670V-48t Summit x480-40G VIM:	4,000 3,791 4,000 3,535 4,000 4,000 3,725 4,000 3,725
MPLS LDP egress LSPs—maximum number of MPLS egress LSPs that can terminate on a switch.	BlackDiamond 8900 xl-series BlackDiamond 8900-40G6X-xm BlackDiamond X8 series E4G-200 E4G-400 Summit X460, X480 Summit X670 Summit X670V-48t Summit x480-40G VIM	7,821 3,791 7,821 3,535 7,525 7,821 3,725 7,821 3,725
MPLS static LSPs—maximum number of static LSPs.	All platforms	100
MSDP active peers—maximum number of active MSDP peers.	BlackDiamond 8000 series BlackDiamond X8 series BlackDiamond 8900 series Summit X460, X480, X650, X670, E4G-400	32 64 64 16
MSDP SA cache entries—maximum number of entries in SA cache.	BlackDiamond 8000 series BlackDiamond X8 series BlackDiamond 8900 series Summit X460, X480, X650, X670, E4G-400	16,000 16,000 16,000 8,000
MSDP maximum mesh groups—maximum number of MSDP mesh groups.	BlackDiamond 8000 series BlackDiamond X8 series BlackDiamond 8900 series Summit X460, X480, X650, X670, E4G-400	8 16 16 4

Table 2: Supported Limits (Continued)

Metric	Product	Limit
Multi-cast listener discovery (MLD) IPv6 multi-cast data sender—maximum number of IPv6 multi-cast streams supported on a switch[i f] **NOTE:** Assumes source-group-vlan mode. For additional limits, see: • Layer-2 IPMC forwarding caches—(IGMP/MLD/PIM snooping) in mac-vlan mode. on page 72 • Layer-2 IPMC forwarding caches— (IGMP/MLD/PIM snooping) in mixed-mode. on page 73	BlackDiamond 8800 a-series BlackDiamond 8800 c-series BlackDiamond 8800 e-series BlackDiamond 8900 c-series BlackDiamond 8900-40G6X-xm BlackDiamond 8900 xl-series BlackDiamond X8 series E4G-200 E4G-400 Summit X150, X250e, X350, X450e Summit X440 Summit X450a Summit X460 Summit X480 Summit X650 Summit X670	750 1,000 250 1,000 1,000 3,000 3,000 1,500 3,000 250 90 750 3,000 3,000 1,500 1,500
Multi-cast listener discovery (MLD) snooping per-VLAN filters—maximum number of VLANs supported in per-VLAN MLD snooping mode.	BlackDiamond a-series BlackDiamond e-series BlackDiamond 8800 c-series BlackDiamond 8900 c-series BlackDiamond 8900 xl-series BlackDiamond 8900-40G6X-xm BlackDiamond X8 series E4G-400, Summit X460 Summit X150, X250e, X350, X450e Summit X450a Summit X480 Summit X440 Summit X650, X670, E4G-200	500 250 1,000 500 2,000 500 500 1,000 250 500 2,000 250 500
Multi-cast listener discovery (MLD)v1 subscribers—maximum number of MLDv1 subscribers per port[j]	BlackDiamond 8800 c-series BlackDiamond xl-series BlackDiamond X8 Series Summit X450a, X450e, X440, SummitStack Summit X460, X480, X650, X670, E4G-400	500 1,500 1,500 750 1,500

Table 2: Supported Limits (Continued)

Metric	Product	Limit
Multi-cast listener discovery (MLD)v1 subscribers—maximum number of MLDv1 subscribers per switch[j]	BlackDiamond 8800 series	10,000
	BlackDiamond X8 series	10,000
	Summit X450a, X450e, X440, SummitStack	5,000
	Summit X460, X480, X650, X670, E4G-400	10,000
Multi-cast listener discovery (MLD)v2 subscribers—maximum number of MLDv2 subscribers per port[j]	BlackDiamond 8800 c-series	500
	BlackDiamond xl series	2,500
	BlackDiamond X8 series	2,000
	Summit X450a, X450e, X440, SummitStack	1,000
	Summit X460, X480, X650, X670, E4G-400	2,000
Multi-cast listener discovery (MLD)v2 subscribers—maximum number of MLDv2 subscribers per switch[j]	BlackDiamond 8800 series	10,000
	BlackDiamond xl series	10,000
	Summit X450a, X450e, X440, SummitStack	5,000
	Summit X460, X480, x650, X670, E4G-400	1,0000
Multi-cast listener discovery (MLD)v2 maximum source per group—maximum number of source addresses per group	All platforms	200
Multi-cast VLAN registration (MVR)—maximum number of MVR senders per switch (IP multi-cast compression disabled). **NOTE:** Assumes source-group-vlan mode.	BlackDiamond 8800 a-series	1,024
	BlackDiamond 8800 c-series	2,048[e]
	BlackDiamond 8000 e-series	500[f]
	BlackDiamond 8900 series	
	8900-10G24X-c modules 8900-G96T-c modules 8900 xl-series 8900-40G6X-xm	2,048[e] 4,096[e] 4,096[e] 3,000[f]
	BlackDiamond X8 series	4,096
	E4G-200	2,048
	E4G-400	500[f]
	Summit X150, X250, X350, X450e	64
	Summit X440	1,024
	Summit X450a	4,096
	Summit X480	2,048
	Summit X460	2,048
	Summit X650	
	VIM3-40G4x	3,000[f]
	Summit X670	
	VIM4-40G4x	3,000[f]

Table 2: Supported Limits (Continued)

Metric	Product	Limit
Multi-cast VLAN registration (MVR)—maximum number of MVR senders per switch (IP multi-cast compression enabled). **NOTE:** Assumes source-group-vlan mode. For additional limits, see: Layer-3 IPMC forwarding caches—(PIM, MVR, PVLAN) in mixed-mode.f on page 73	BlackDiamond 8800 a-series BlackDiamond 8800 c-series BlackDiamond 8000 e-series BlackDiamond 8900 c-series BlackDiamond 8900 xl-series BlackDiamond X8 series 8900-40G6X-xm module Summit X150, X250e, X350, X450e Summit X440 Summit X450a Summit X460, E4G-400 Summit X480 Summit X650 VIM3-40G4x Summit X670 VIM4-40G4x	2,000[f] 6,000[f] 500[f] 6,000[f] 12,000[b] 6,000[f] 3,000[f] 500[f] 192[f] 2,000[f] 6,000[f] 12,000[b] 6,000[f] 3,000[f] 3,000[f]
Network login—maximum number of clients being authenticated on MAC-based VLAN enabled ports.	BlackDiamond 8000 series (clients per module/per system) BlackDiamond X8 series Summit series	1,024 1,024 1,024
Network login—maximum number of dynamic VLANs.	All platforms (except Summit X430) Summit X430	2,000 1,024
Network login VLAN VSAs— maximum number of VLANs a client can be authenticated on at any given time.	All platforms	10
OSPF adjacencies—maximum number of supported OSPF adjacencies.	BlackDiamond 8000 series BlackDiamond 8900 xl-series BlackDiamond X8 Series Summit X250e, X460, X650, X670 Summit X440 Summit X480 E4G-400, E4G-200	128 255 255 128 128 255 128
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 and OSPFv3.	All platforms, except Summit X440	2, 4, or 8

Table 2: Supported Limits (Continued)

Metric	Product	Limit
OSPF external routes—recommended maximum number of external routes contained in an OSPF LSDB.	BlackDiamond 8000 series BlackDiamond 8900 xl-series BlackDiamond X8 series Summit X250e, X450a, X460, X650, X670 Summit X480 E4G-400 E4G-200	20,000 130,000 20,000 5,000 130,000 5,000 5,000
OSPF inter- or intra-area routes—recommended maximum number of inter- or intra-area routes contained in an OSPF LSDB with one ABR in OSPF domain.	BlackDiamond 8000 series BlackDiamond 8900 xl-series BlackDiamond X8 series Summit X250e, X450a, X460, X650, X670 E4G-400 Summit X480	7,000 7,000 7,000 2,000 2,000 7,000
OSPF routers in a single area—recommended maximum number of routers in a single OSPF area.	BlackDiamond 8000 series BlackDiamond 8900 xl-series BlackDiamond X8 series Summit X250e, X450a, X460, X650, X670 Summit X480 E4G-400	100 200 100 50 200 50
OSPF subnets on a single router—recommended maximum number of OSPF routed subnets on a switch.	All platforms with Core license or higher	400
OSPF virtual links—maximum number of supported OSPF virtual links.	All platforms with Core license or higher	32
OSPFv2 links—maximum number of links in the router LSA.	All platforms	419
OSPFv3 active interfaces—maximum number of OSPFv3 active interfaces.	All platforms with Advanced Edge license	4
OSPFv3 areas—as an ABR, the maximum number of supported OSPFv3 areas.	All platforms with Core license or higher	16
OSPFv3 external routes—recommended maximum number of external routes.	BlackDiamond 8000 series BlackDiamond X8 series BlackDiamond 8900 xl-series Summit X450a, X460, X650, X670 Summit X480 E4G-400	10,000 10,000 60,000 10,000 60,000 10,000

Table 2: Supported Limits (Continued)

Metric	Product	Limit
OSPFv3 interfaces—maximum number of OSPFv3 interfaces.	BlackDiamond 8000 series	256
	BlackDiamond X8 series	256
	BlackDiamond 8900 xl-series	384
	Summit X450a, X460, X650, X670	128
	Summit X480	384
	E4G-400	128
OSPFv3 inter- or intra-area routes—recommended maximum number of inter- or intra-area routes.	BlackDiamond 8000 series	6,000
	BlackDiamond X8 series	6,000
	BlackDiamond 8900 xl-series	6,000
	Summit X450a, X460, X650, X670	3,000
	Summit X480	6,000
	E4G-400	3,000
OSPFv3 neighbors—maximum number of OSPFv3 neighbors.	BlackDiamond 8000 series	64
	BlackDiamond X8 series	64
	BlackDiamond 8900 xl-series	128
	Summit X450a, X460, X650, X670	64
	Summit X480	128
	E4G-400	64
OSPFv3 virtual links—maximum number of OSPFv3 virtual links supported.	All platforms with Core license or higher	16
PIM IPv4 snooping—maximum number of (S,G) entries programmed in the hardware (IP multi-cast compression disabled). **NOTE:** Assumes source-group-vlan mode.	BlackDiamond 8800 c-series	2,048[e]
	BlackDiamond 8000 e-series	500[e]
	BlackDiamond 8900 series	
	8900-10G24X-c modules	2,048[e]
	8900-G96T-c modules	4,096[e]
	8900 xl-series	4,096[e]
	8900-40G6X-xm	3,000[f]
	BlackDiamond X8 series	4,096
	E4G-200	2,048
	E4G-400	2,048
	Summit X150, X250e, X350, X450e	500[f]
	Summit X440	64
	Summit X450a	1,024
	Summit X460	2,048
	Summit X480	4,096
	Summit X650	2,048
	VIM3-40G4x	3,000[f]
	Summit X670	
	VIM4-40G4x	3,000[f]

Table 2: Supported Limits (Continued)

Metric	Product	Limit
PIM IPv4 snooping—maximum number of (S,G) entries programmed in the hardware (IP multi-cast compression enabled). **NOTE:** Assumes source-group-vlan mode. For additional limits, see: • Layer-2 IPMC forwarding caches—(IGMP/MLD/PIM snooping) in mac-vlan mode. on page 72 • Layer-2 IPMC forwarding caches— (IGMP/MLD/PIM snooping) in mixed-mode. on page 73	BlackDiamond 8800 a-series BlackDiamond 8800 c-series BlackDiamond 8000 e-series BlackDiamond 8900 c-series BlackDiamond 8900 xl-series BlackDiamond X8 series E4G-200 E4G-400 8900-40G6X-xm Summit X150, X250e, X350, X450e Summit X440 Summit X450a Summit X480 Summit X460 Summit X650 VIM3-40G4x Summit X670 VIM4-40G4x	2,000[f] 6,000[f] 500[f] 6,000[f] 12,000[b] 6,000[f] 3,000[f] 6,000[f] 3,000[f] 500[f] 192[f] 2,000[f] 12,000[b] 6,000[f] 6,000[f] 3,000[f] 3,000[f]
PIM IPv4—maximum routes—maximum number of (S,G) entries installed in the hardware (IP multi-cast compression disabled). **NOTE:** Assumes source-group-vlan mode.	BlackDiamond 8800 c-series BlackDiamond 8000 e-series BlackDiamond 8900 series 8900-10G24X-c modules 8900-G96T-c modules 8900 xl-series 8900-40G6X-xm BlackDiamond X8 series E4G-200 E4G-400 Summit X150, X250e, X350, X450e Summit X440 Summit X450a Summit X480 Summit X460 Summit X650 VIM3-40G4x Summit X670 VIM4-40G4x	2,048[e] 500[f] 2,048[e] 4,096[e] 4.096[e] 3,000[f] 4,094 2,048 2,048 500[f] 64[f] 1,024 4,096 2,048 2,048 3,000[f] 3,000[f]

Table 2: Supported Limits (Continued)

Metric	Product	Limit
PIM IPv4—maximum routes—maximum number of (S,G) entries installed in the hardware (IP multi-cast compression enabled). **NOTE:** Assumes source-group-vlan mode. For additional limits, see: Layer-3 IPMC forwarding caches—(PIM, MVR, PVLAN) in mixed-mode.f on page 73	BlackDiamond 8800 a-series BlackDiamond 8800 c-series BlackDiamond 8000 e-series BlackDiamond 8900 c-series BlackDiamond 8900 xl-series BlackDiamond X8 series E4G-200 E4G-400 8900-40G6X-xm modules Summit X150, X250e, X350, X450e Summit X440 Summit X450a Summit X480 Summit X460 Summit X650 VIM3-40G4x Summit X670 VIM4-40G4x	2,000[f] 6,000[f] 500[f] 6,000[f] 12,000[b] 6,000[f] 3,000[f] 6,000[f] 3,000[f] 500[f] 192 2,000[f] 12,000[b] 6,000[f] 6,000[f] 3,000[f] 3,000[f]
PIM IPv4-SSM (maximum SSM routes)—maximum number of (S,G) entries installed in the hardware with PIM SSM configuration (IP multi-cast compression disabled). **NOTE:** Assumes source-group-vlan mode.	BlackDiamond 8800 c-series BlackDiamond 8000 e-series BlackDiamond 8900 series 8900-10G24X-c modules 8900-G96T-c modules 8900 xl-series 8900-40G6X-xm BlackDiamond X8 series E4G-200 E4G-400 Summit X150, X250e, X350, X450e Summit X440 Summit X450a Summit X480 Summit X460 Summit X650 VIM3-40G4x Summit X670 VIM4-40G4x	2,048[e] 500[f] 2,048[e] 4,096[e] 15,000 3,000[f] 4,094 2,048 2,048 500[f] 64 1,024 4,096 2,048 2,048 3,000[f] 3,000[f]

Table 2: Supported Limits (Continued)

Metric	Product	Limit
PIM IPv4-SSM (maximum SSM routes)—maximum number of (S,G) entries installed in the hardware with PIM SSM configuration (IP multi-cast compression enabled). **NOTE:** Assumes source-group-vlan mode. For additional limits, see: Layer-3 IPMC forwarding caches—(PIM, MVR, PVLAN) in mixed-mode.f on page 73	BlackDiamond 8800 a-series BlackDiamond 8800 c-series BlackDiamond 8000 e-series BlackDiamond 8900 c-series BlackDiamond 8900 xl-series BlackDiamond X8 series E4G-200 E4G-400 8900-40G6X-xm Summit X150, X250e, X350, X450e Summit X440 Summit X450a Summit X480 Summit X460 Summit X650 VIM3-40G4x Summit X670 VIM4-40G4x	2,000[f] 6,000[f] 500[f] 6,000[f] 12,000[b] 6,000[f] 3,000[f] 6,000[f] 3,000[f] 500[f] 192[f] 2,000[f] 12,000[b] 6,000[f] 6,000[f] 3,000[f] 3,000[f]
PIM IPV6 (maximum routes)—maximum number of (S,G) entries installed in the hardware. **NOTE:** Assumes source-group-vlan mode.	BlackDiamond 8800 a-series BlackDiamond 8800 c-series BlackDiamond 8800 e-series BlackDiamond 8900 c-series BlackDiamond 8900-40G6X-xm BlackDiamond 8900 xl-series BlackDiamond X8 series E4G-200 E4G-400 Summit X150, X250e, X350, X450e Summit X440 Summit X450a Summit X460 Summit X480 Summit X650 Summit X670	750 1,000 250 1,000 1,000 3,000 3,000 1,500 3,000 250 90 750 3,000 3,000 1,500 1,500
PIM IPv4 (maximum interfaces)—maximum number of PIM active interfaces.	All platforms	512
PIM IPv4 (maximum interfaces)—maximum number of PIM snooping enabled interfaces.	All platforms	256

Table 2: Supported Limits (Continued)

Metric	Product	Limit
PIM IPv4 Limits—maximum number of multi-cast groups per rendezvous point	All platforms	180
PIM IPv4 Limits—maximum number of multi-cast sources per group	All platforms	175
PIM IPv4 Limits—maximum number of dynamic rendezvous points per multi-cast group	All platforms	145
PIM IPv4 Limits—static rendezvous points	All platforms	32
PIM IPv6 (maximum interfaces)—maximum number of PIM active interfaces	All platforms	512
PIM IPv6 Limits—maximum number of multicast group per rendezvous point	All platforms	70
PIM IPv6 Limits—maximum number of multicast sources per group	All platforms	43
PIM IPv6 Limits—maximum number of dynamic rendezvous points per multicast group	All platforms	64
PIM IPv6 Limits—maximum number of secondary address per interface	All platforms	70
PIM IPv6 Limits—static rendezvous points	All platforms	32
Policy-based routing (PBR) redundancy—maximum number of flow-redirects.	All platforms	256[k]
Policy-based routing (PBR) redundancy—maximum number of next hops per each flow-direct.	All platforms	32[k]
Private VLANs—maximum number of subscribers. Assumes a minimum of one port per network and subscriber VLAN.	BlackDiamond 8800 a-, c-, e-, xl-series with eight modules of 48 ports 8900-G96T-c modules BlackDiamond X8 series Summit series	 383 767 767 One less than the number of available user ports

Table 2: Supported Limits (Continued)

Metric	Product	Limit
Private VLANs—maximum number of private VLANs with an IP address on the network VLAN. **NOTE:** This limit is dependent on the maximum number of private VLANs in an L2-only environment if the configuration has tagged and translated ports.	All platforms	512
Private VLANs—maximum number of private VLANs in an L2-only environment.	BlackDiamond 8800 a-, c-, e-series BlackDiamond 8900 series BlackDiamond X8 series E4G-200 E4G-400 Summit X440 Summit X250e, X450a, X450e Summit X480, X650 Summit X670 Summit X460	384 2,046 2,046 597 1,280 127 384 2,046 597 820
PTP/1588v2 Clock Ports	E4G Platforms	32 for boundary clock 1 for ordinary clock
PTP/1588v2 Clock Instances	E4G Platforms	2 combinations: • Transparent clock + ordinary clock • Transparent clock + boundary clock
PTP/1588v2 Unicast Static Slaves	E4G Platforms	40 entries per clock port
PTP/1588v2 Unicast Static Masters	E4G Platforms	10 entries per clock type
Route policies—suggested maximum number of lines in a route policy file.	All platforms	10,000
RIP neighbors—maximum number of RIP neighbors.	E4G-200	256

Table 2: Supported Limits (Continued)

Metric	Product	Limit
RIP interfaces on a single router—recommended maximum number of RIP routed interfaces on a switch.	BlackDiamond 8000 series BlackDiamond X8 series BlackDiamond 8900 xl-series Summit X250e, X450a, X440 Summit X460 Summit X480 Summit X650, X670 E4G-400	256 256 384 128 256 384 256 256
RIPng learned routes—maximum number of RIPng routes.	BlackDiamond 8000 series BlackDiamond X8 series BlackDiamond 8900 xl-series Summit X250e, X450a Summit X480 Summit X460, X650, X670 E4G-400 E4G-200	3,000 3,000 5,000 1,500 5,000 3,000 3,000 10,000
RSVP-TE interfaces—maximum number of interfaces.	All platforms	32
RSVP-TE ingress LSPs— maximum number of ingress LSPs.	All platforms	2,000
RSVP-TE egress LSPs—maximum number of egress LSPs.	All platforms	2,000
RSVP-TE transit LSPs—maximum number of transit LSPs.	All platforms	2,000
RSVP-TE paths—maximum number of paths.	All platforms	1,000
RSVP-TE profiles—maximum number of profiles.	All platforms	1,000
RSVP-TE EROs—maximum number of EROs per path.	All platforms	64
Spanning Tree (maximum STPDs)—maximum number of Spanning Tree Domains on port mode EMISTP.	All platforms (except Summit X430) Summit X430	64 16

Table 2: Supported Limits (Continued)

Metric	Product	Limit
Spanning Tree PVST+—maximum number of port mode PVST domains. **NOTE:** • Maximum of 10 active ports per PVST domain when 256 PVST domains are configured. • Maximum of 7 active ports per PVST domain when 128 PVST domains are configured.	BlackDiamond X8 and 8900 series switches Summit X670 Summit X460, X480, X650, X440 Summit X430 E4G-400	256 256 128 50 128
Spanning Tree—maximum number of multiple spanning tree instances (MSTI) domains.	All platforms (exceptc Summit X430) Summit X430	64 5
Spanning Tree—maximum number of VLANs per MSTI. **NOTE:** Maximum number of 10 active ports per VLAN when all 500 VLANs are in one MSTI.	All platforms (except Summit X460, X430, and E4G-400) Summit X460 and E4G-400 Summit X430	500 600 100
Spanning Tree—maximum number of VLANs on all MSTP instances.	All platforms (except Summit X460, Summit X430, and E4G-400) Summit X460 and E4G-400 Summit X430	1,000 1,024 200
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 (except Summit X430) Summit X430	4,096 1,024
Spanning Tree (maximum VLANs)—maximum number of STP protected VLANs (dot1d and dot1w).	BlackDiamond X8 and 8900 series Summit X460 and E4G-400 Summit X430 All other platforms	1,024 600 128 560
SSH (number of sessions)—maximum number of simultaneous SSH sessions.	All platforms	8
Static MAC multi-cast FDB entries—maximum number of permanent multi-cast MAC entries configured into the FDB.	BlackDiamond 8000 a-, c-, e-, xl-series BlackDiamond X8 series Summit X150, X350, X250e, X450a, X450e, X460, X480, X650, X670, X430 E4G-400	1,024 1,024 1,024 1,024

Table 2: Supported Limits (Continued)

Metric	Product	Limit
Syslog servers—maximum number of simultaneous syslog servers that are supported.	All platforms	4
Telnet (number of sessions)—maximum number of simultaneous Telnet sessions.	All platforms	8
Virtual routers—maximum number of user-created virtual routers that can be created on a switch. **NOTE:** Virtual routers are not supported on Summit X150, X250e, X350, X440, X450a, and X450e series switches.	BlackDiamond 8000 c-, xl-, xm-series BlackDiamond X8 series E4G-200, E4G-400 Summit X460, X480, X650, X670	63 63 63 63
Virtual router forwarding (VRFs)—maximum number of VRFs that can be created on a switch. **NOTE:** *The Summit X430 does not support user user VRFs.	BlackDiamond 8000 xl- and xm-series BlackDiamond 8000 c-series BlackDiamond X8 series Summit X460, X480, X650, X670 Summit X430* E4G-400 E4G-200	190 64 190 190 N/A 190 125
VRF forwarding instances—number of non-VPN VRFs that can be created on a switch.	BlackDiamond 8000 c-, xl-, xm-series Summit X460, X480, X650, X670 E4G-400	190 190 190
Virtual router protocols per VR—maximum number of routing protocols per VR.	All platforms	8
Virtual router protocols per switch—maximum number of VR protocols per switch.	All platforms	64
VLAN aggregation—maximum number of port-VLAN combinations on any one superVLAN and all of its subVLANs.	All platforms (except Summit X440) Summit X440	1,000 256
VLANs—includes all VLANs.	All platforms	4,094
VLANs (Layer 2)—maximum number of Layer 2 VLANs.	All platforms	4,094
VLANs (Layer 3)—maximum number of Layer 3 VLANs.	BlackDiamond X8 series All BlackDiamond 8000 series and Summit family switches with Edge license or higher Summit X440	512 512 254

Table 2: Supported Limits (Continued)

Metric	Product	Limit
VLANs (maximum active port-based)—(Maximum active ports per VLAN when 4,094 VLANs are configured with default license)	Summit X670, X650, X480,X460, E4G-400 Summit X440 E4G-200 Summit X450e, X350, X250e, X150 Summit X450a, X430	32 32 16 12 2 1
VLANs (maximum active protocol-sensitive filters)—number of simultaneously active protocol filters in the switch.	All platforms	15
VLAN translation—maximum number of translation VLANs. Assumes a minimum of one port per translation and member VLAN.	BlackDiamond 8000 a-, c-, e-, xl-series with eight modules of 48 ports 8900-G96T-c modules BlackDiamond X8 series Summit X450a and X450e, group of 24 ports with two-port option cards without option cards Summit series	 383 767 767 25 23 One less than the number of available user ports
VLAN translation—maximum number of translation VLAN pairs with an IP address on the translation VLAN. **NOTE:** This limit is dependent on the maximum number of translation VLAN pairs in an L2-only environment if the configuration has tagged and translated ports.	All platforms	512
VLAN translation—maximum number of translation VLAN pairs in an L2-only environment.	BlackDiamond 8800 a-, c-, e-series BlackDiamond 8900 xl-series BlackDiamond X8 series Summit X460 E4G-400, E4G-200 Summit X440 Summit X250e, X450a, X450e Summit X480, X650, X670 Summit X430	384 2,046 2,046 2,000 2,000 512 384 2,046 100

Table 2: Supported Limits (Continued)

Metric	Product	Limit
VPLS: VCCV (pseudo wire Virtual Circuit Connectivity Verification) VPNs—maximum number of VCCV enabled VPLS VPNs.	All platforms	16
VPLS: MAC addresses—maximum number of MAC addresses learned by a switch.	BlackDiamond 8900 xl-series BlackDiamond 8900-40G6X-xm BlackDiamond X8 series E4G-200, E4G-400 Summit X460 Summit X480 Summit X670, Summit X670V-48t Summit X480-40G VIM	512,000 128,000 128,000 32,000 32,000 512,000 128,000 121,000
VPLS VPNs—maximum number of VPLS virtual private networks per switch.	BlackDiamond 8900 xl-series BlackDiamond 8900-40G6x-xm BlackDiamond X8 series E4G-200, E4G-400 Summit 460 Summit X480, X670, Summit X670V-48t Summit X480-40G VIM	1,023 1,023 1,023 1,000 1,000 1,023 1,023
VPLS peers—maximum number of VPLS peers per VPLS instance.	Summit X480 Summit X460 BlackDiamond 8900 xl-series BlackDiamond 8900-40G6x-xm Summit X670 Summit X670V-48t, Summit X480-40G VIM BlackDiamond X8 series E4G-200, E4G-400	64 32 64 64 32 64 64 32
VPLS pseudo wires—maximum number of VPLS pseudo wires per switch.	BlackDiamond 8900 xl-series BlackDiamond 8900-40G6X-xm BlackDiamond X8 series E4G-200, E4G-400 Summit X460 Summit X480 Summit X670 Summit X670V-48t Summit X480-40G VIM	7,800 4,000 7,800 1,000 1,000 7,800 4,000 7,800 3,716

Table 2: Supported Limits (Continued)

Metric	Product	Limit
Virtual Private Wire Service (VPWS): VPNs—maximum number of virtual private networks per switch.	Summit X460 Summit X480 Summit X480-40G VIM Summit X670 Summit X670V-48t BlackDiamond 8900 xl-series BlackDiamond 8900-40G6X-xm BlackDiamond X8 series E4G-200, E4G-400	1,000 4,000 2,047 2,047 4,000 4,000 2,047 4,000 1,000
VRRP (maximum instances)—maximum number of VRRP instances for a single switch.	BlackDiamond X8 series BlackDiamond 8800 c-series MSM-48c BlackDiamond 8900 xl-series 8900-MSM128 All other platforms with Advanced Edge license or higher	255 255 255 128
VRRP (maximum VRID)—maximum number of unique VRID numbers per switch.	All platforms with Advanced Edge license or higher	7
VRRP (maximum VRIDs per VLAN)—maximum number of VRIDs per VLAN.	All platforms with Advanced Edge license or higher	7
VRRP (maximum ping tracks)—maximum number of ping tracks per VLAN.	All platforms with Advanced Edge license or higher	8
VRRP (maximum ping tracks)—maximum number of ping tracks per VRRP Instance under 128 VRRP instances. **Hello interval:** 100 milliseconds **Hello interval:** 1 second	All platforms with Advanced Edge license or higher	 2 4
VRRP (maximum iproute tracks)—maximum number of IP route tracks per VLAN.	All platforms with Advanced Edge license or higher	8
VRRP—maximum number of VLAN tracks per VLAN.	All platforms with Advanced Edge license or higher	8
XML requests—maximum number of XML requests per second. **NOTE:** Limits are dependent on load and type of XML request. These values are dynamic ACL data requests.	BlackDiamond 8800 c-series with 100 DACLs with 500 DACLs BlackDiamond 8900 series with 100 DACLs with 500 DACLs Summit X450a, X480, X650, X670 with 100 DACLs with 500 DACLs	 10 3 10 3 4 1

Table 2: Supported Limits (Continued)

Metric	Product	Limit
XNV authentication—maximum number of VMs that can be processed (combination of local and network VMs).	All platforms	2,048
XNV database entries—maximum number of VM database entries (combination of local and network VMs).	All platforms	16,000
XNV database entries—maximum number of VPP database entries (combination of local and network VPPs).	All platforms	2,048
XNV dynamic VLAN—Maximum number of dynamic VLANs created (from VPPs /local VMs)	All Platforms	2,048
XNV local VPPs—maximum number of XNV local VPPs.	All platforms (except Summit X430) Ingress Egress Summit X430 Ingress	 2,048 512 1,024
XNV policies/dynamic ACLs—maximum number of policies/ dynamic ACLs that can be configured per VPP.[l]	All platforms (except Summit X430) Ingress Egress Summit X430 Ingress	 8 4 8
XNV network VPPs—maximum number of XNV network VPPs.[l]	All platforms (except Summit X430) Ingress Egress Summit X430 Ingress	 2,048 512 1,024

a. The table shows the total available.
b. Limit depends on setting configured for `configure forwarding external-tables`.
c. When there are BFD sessions with minimal timer, sessions with default timer should not be used.
d. Effective capacity varies based on actual MAC addresses and VLAN IDs used and hash algorithm selected.
e. Applies only if all enabled BlackDiamond 8000 I/O modules are BlackDiamond 8000 c-, xl-, or xm-series modules.
f. Effective capacity varies based on actual IP addresses and hash algorithm selected, but is higher for BlackDiamond 8000 c-, xl-, xm-series modules, BlackDiamond X8, E4G cell site routers, and Summit X460, X480, X650, and X670 switches compared to BlackDiamond 8800 a-series and 8000 e-series modules and Summit X250e, X450e, and X450a switches.
g. For the MVR feature in the BlackDiamond X8 series switches, the number of senders applies only when there are few egress VLANs with subscribers. If there are many VLANs with subscribers, the limit is substantially less. Only 500 senders are supported for 100 VLANs. It is not recommended to exceed these limits.
h. The limit depends on setting configured with `configure iproute reserved-entries`.
i. The IPv4 and IPv6 multi-cast entries share the same hardware tables, so the effective number of IPv6 multi-cast entries depends on the number of IPv4 multi-cast entries present and vice-versa.
j. If IGMP and MLD are simultaneously configured on the switch, the number of effective subscribers supported would be appropriately lessened.
k. Sum total of all PBR next hops on all flow redirects should not exceed 1024.

l. The number of XNV authentications supported based on system ACL limitations.

3 Open Issues, Known Behaviors, and Resolved Issues

This chapter describes items needing further clarification and behaviors that might not be intuitive. It also includes the items that have been resolved..

NOTE

Extreme Networks is transitioning to a new software defect numbering system. Previously, software defect ID numbers were prefaced with the letters “PD”; they will now be prefaced with “XOS.” During this transition period, some software defects will have the old format ID and some will have the new one.

This chapter contains the following sections:

Open Issues

The following are the open issues for supported features in ExtremeXOS 15.3.5-Patch1-3.

Table 3: Open Issues, Platform-Specific and Feature Issues

ID Number	Description
General	
xos0058750	Neighbor discovery packets are duplicated in L2 VLANs when IPv6 addresses are configured for other VLANs that do not have any ports.
xos0060909	In UPM profiles the variable EVENT.TIME incorrectly has the current time rather than the time when the event was queued/ triggered.
BlackDiamond 8800 Series Switches	
xos0057030	ACL process ends unexpectedly after executing the command `refresh access-list network-zone`.
xos0050728	After installing ExtremeXOS 15.3.1.1, backup MSMs fails to sync with MSM A and the following error appears on MSM A: "Failed to checkpoint configuration: timed out (after 500 seconds) while waiting for configuration checkpoint save operation to finish (hal is still not saved)".
xos0050633	When booting up, BlackDiamond 8900-10G8X-xl series switches go to failed state before coming to operational state and the following error message appears: "<Erro:HAL.Port.Error> MSM-A: Unable to configure DWDM channel to the transceiver for port 2:7 (-1) This issue is seeing only with v15_3_0_25 build. This issue is not seen with v15_2_2_7 build".
xos0050757	When configuring dynamic L2 PBR with port, the following error appears: "EgressACL_Broadcom: <Erro:HAL.IPv4ACL.Error> MSM-A: ACL filter install failed on vlan *, port 5:1, rule "rule228" index 129, No resources for operation (rule)".
xos0050774	When VMT is enabled and VM is authenticated, the following error appears: "freeDynamicRule: ERROR: Can't free Rule index (-14855)... still inuse" and "bindDynamicRule: ERROR: Can't find the dynamic rule (4294952451)".

Table 3: Open Issues, Platform-Specific and Feature Issues (Continued)

ID Number	Description
BlackDiamond X8 Series Switches	
xos0050820	RIP process ends unexpectedly with signal 11
xos0050452	Cannot create 256 VRRPv3-enabled IPv6 interfaces and 10 non-VRRPv3-enabled interfaces on BlackDiamond X8 series switches and Summit X670-48T and X650 series switches.
xos0054152	IP addresses of network-zone appear in reverse order in the output of the `show access-list port <port_no> detail` command.
xos0050387	Process BGP consumes 99% of the CPU after restarting process BGP.
Summit Series Switches	
xos0050889	After rebooting 8-node Summit X440-24x stacks after creating 4,094 VLANs, systems stops working.;
xos0050319	When ESRP and ELRP are enabled with all the ports added to the master VLAN, the master switch stops working after receiving a `show vlan MasterVlan` command. The state of the ESRP master switch switches between master and slave for some domains.
xos0050890	When disabling/enabling/powering down a peer switch, the master node of an 8-node Summit X440-24x stack goes down unexpectedly.
xos0050918	While sending unknown traffic from isolated VLANs with MAC 01, VLANs are flooded and FDB is learned. While sending L2 traffic from non-isolated VLANs to isolated VLANs, traffic is dropped, as expected. After clearing the FDB and repeating the above process, expected flooding on network VLANs does not occur.
xos0053717	Transmit packet counters for RSVP-LSPs do not work on Summit X460 series switches.
SummitStack	
xos0051147	The 40G QSFP+ SR4 link on the port by default is in 1x40G mode on Summit X670v-48x stacks, but it should appear only in channel one. This issue does not occur in the chassis or standalone switch.
xos0049064	Kernel error occurs on Summit X440 series switches slots when enabling jumbo frames in stack.
xos0058133	SummitStacks use slot MAC addresses in DHCP packets when enabling DHCP on Management VLAN.
E4G-200 and 400 Cell Site Routers	
xos0050607	Ping fails through VPN after creating 125th VPN VRF.
xos0050133	After dynamically changing the route-distinguisher value in PE-1 node, remote PE-2 fails to advertise the updated VPNv4 routes as IPv4 routes to its connected CE.
AVB	
xos0048963	Egress rate-limiting is allowed on MSRP enabled ports.
xos0050236	AVB traffic fails on user-VR.

Table 3: Open Issues, Platform-Specific and Feature Issues (Continued)

ID Number	Description
BGP	
xos0050794	DCBGP process ends unexpectedly with signal 11 when rebooting or issuing the `command disable/enable bgp` on neighboring switches
xos0049687	Aggregate policy is not functioning in BGP.
xos0050130	BGPv4/v6 is not preserving routes when GR is enabled.
ERPS	
xos0050463	Duplicate IPv6 addresses are detected when they don't exist when disabling/enabling ports between ESRP master and L2 switch.
xos0049959	Using ESPR priority-ports-track-mac algorithm, BlackDiamond X8 series switches running ExtremeXOS 15.2.2 have dual slave state. This is not seen in Summit switches.
xos0049974	On BlackDiamond series switches, the `show esrp domain1` command shows an incorrect summary when one ESRP VLAN is configured with track ping and also track route.
xos0049944	IPv6 address for ESRP domain cannot be configured and it shows 0.0.0.0 as VID, but when IPv4 address is also configured along with IPv6 then it shows IPv4 address as VID. This issue occurs in ExtremeXOS 15.3 and 15.2.
ESRP	
xos0049979	On BlackDiamond X8 and BlackDiamond 8800 series switches, the ESRP state is a slave state when the maximum number of ESRP domain and track ping can be configured (256). However, the expected master state is seen on E4G-200 cell site routers. This issue occurs with ExtremeXOS 15.3 and 15.2.2.
MPLS	
xos0049742	The command `show iproute mpls` shows only seven routes from MPLS, when there are eight static LSPs configured.
xos0050376	On Summit X480 series switches, pings to neighboring router loopback addresses fail when no source is entered in the ping command.
VRRP	
xos0050288	VRRPv3 remains in backup state for 60 seconds.
XNV	
xos0050772	The command `show access-list dynamic counter` does not display the correct packets expected for VM MAC addresses.
xos0050771	The command `show access-list dynamic counters` does not display the complete MAC address of VMs and it may not be possible to read the counters correctly from the output.
xos0050305	If a dynamic VLAN is added to OSPF, the OSPF configuration is retained even after the dynamic VLAN is removed.

Corrections to Open Issues Table

The following table lists open issues that were erroneously listed in of the previous revision of this release note for ExtremeXOS 15.3. These issues have been removed from the current Table 3.

Table 4: Erroneously Listed Issues in the Open Table of ExtremeXOS 15.3

ID Number	Description	Reason Issues Was Removed
PD4-1842342815, PD4-1291631579	When working in network login, after a dot1x client logs out, the port is not moved to a MAC-based VLAN.	Problem was fixed in an earlier ExtremeXOS release.
PD4-3286100221	ACL_PERSISTANCE_RETRY - Verifying persistent Dynamic ACLs having higher priority compared to policy-based ACL, after save/ reboot, traffic failed after reboot.	Cannot reproduce this problem.
PD4-3629988087	Program HAL ends unexpectedly with signal 11 (segmentation fault).	Cannot reproduce this problem.
PD4-3447899751	RIP process ends unexpectedly with signal 11.	Cannot reproduce this problem.
PD4-3690474911	Static routes with tunnels as gateways become inactive after failover to backup MSM. The same issue occurs while rebooting GRE/6in4 tunnel end point. **Workaround:** Disable GRE tunnelname, and then enable GRE tunnelname. Routes will appear.	Cannot reproduce this problem..
PD4-3393310741	Process ChkLst_ACL ends unexpectedly with signal 11: #0 0x00430528 in aclRuleAppl_t_config (context=0x0, objIn=0x7fff55a0, appl=5273952) at acl_cli.c:5277 5277 index = ACL_ZONE_INDEX (appl,priority);	Cannot reproduce this problem..
PD4-2330473390, PD4-2012884711	The following critical message may be logged followed by a system crash when making a configuration change to a private VLAN: `System call ioctl failed failed: informCfgVlanAddPorts and 15`	Problem was fixed in an earlier ExtremeXOS release.

Table 4: Erroneously Listed Issues in the Open Table of ExtremeXOS 15.3

ID Number	Description	Reason Issues Was Removed
PD4-2255170647	After disabling and re-enabling a port using the `clear elsm port <port no> auto-restart` command, the ELSM state does not come up. **Workaround:** Disable and then enable the port.	Problem will not be fixed.
PD4-2483785534, PD4-2483785491	The option end-point should not be included in the `configure vlan <vlan name> add ports <port no>` tagged private-vlan command.	Problem was fixed in an earlier ExtremeXOS release.
PD4-3223230501	The command `run msm fail-over` or `run fail-over` removes NTP configuration on a VLAN when NTP and DAD are enabled on the same VLAN.	Duplicate of PD4-3227396996 (in the Resolved table for ExtremeXOS 15.3, Table 29 on page 156)
PD4-3238152635	NTP and DAD cannot co-exist. If you enable NTP and DAD on the same VLANs, save the configuration, and then reboot the switch, the NTP configuration for VLANs is removed when switch comes up.	Problem was fixed in an earlier ExtremeXOS release.
PD4-3106307537	While start esvt test, existing FDB entry for the peer node is cleared from `show fdb` table automatically and port numbers connected to peer node are not showing in `show iparp` table. This floods traffic across all ports configured in service VLAN.	Not found to be a problem.
PD4-3325786333	CLI execution fails and produces the following error: "enable sharing 6 grouping 6 10 algorithm address-based lacp" <Erro:HAL.Port.Error> : Failed to disable static mac move drop on port 10.< > * (Engineering debug) X450e-24p.576 # - 21:14:38 < Illegal Line is 12/08/2012 21:14:37.32 <Erro:HAL.Port.Error> : Failed to disable static mac move drop on port 10.	Problem was fixed in ExtremeXOS 15.3 before it was released.
PD4-3273653251	Packet loss is occurring after deleting/recreating the GRE tunnel.	Problem was fixed in ExtremeXOS 15.3 before it was released.
PD4-3272987031	In the *ExtremeXOS Concepts Guide*, the configuration example given for ELSM needs to be corrected.	Problem was fixed in ExtremeXOS 15.3 before it was released.

Table 4: Erroneously Listed Issues in the Open Table of ExtremeXOS 15.3

ID Number	Description	Reason Issues Was Removed
PD4-3254256795	VRRP transition is not happening immediately when its receiving advertisements with priority zero.	Not found to be a problem.
PD4-3339092117	After enabling the trunk VLAN v7 at both FHR and RP, the output of the command `show pim cache detail` at RP does not update the source entry (S) flag for the source from FHR.	Problem was fixed in ExtremeXOS 15.3 before it was released.
PD4-3271203970	Debug message appears on console when enabling OpenFlow: "Nov 15 12:27:39|00001|lockfile|INFO|/var/run/openvswitch/.conf.db.~lock~: lock file does not exist, creating"	Problem was fixed in ExtremeXOS 15.3 before it was released.
PD4-3271246241	The command `show mpls l3vpn label received` displays no output.	Problem was fixed in ExtremeXOS 15.3 before it was released.
PD4-3328261697	L3 - Expected parameters failed to show up in the command `show iparp` in L3 module. Parameter details are : "Rejected Count" "Rejected Port" / "Dup IP Addr". This worked fine until ExtremeXOS v15.3.	Cannot reproduce this problem.
PD4-1599215746	Ping fails for remote loopback addresses.	Cannot reproduce this problem.
PD4-3303209931	rtmgr process ends unexpectedly with signal 11 while rebooting neighboring switches.	Problem was fixed in ExtremeXOS 15.3 before it was released.
PD4-3298871993	BGP aggregation is not working after withdraw and advertise of routes.	Cannot reproduce this problem.
PD4-3322820940	Traffic loss is occurring in OSPF-Graceful restart.	Not found to be a problem.
PD4-2501758416	Process route manager hits 99% CPU during link flap of LAG port in a PIM enabled VLAN.	Problem was fixed in ExtremeXOS 15.1.1.
PD4-3286134421	After restarting ports, the following errors occur in MSM-B: <Erro:HAL.SM.Error> MSM-B: aspenSmIpmcAddEgressPort: group does not exist 11/21/2012 16:59:53.70 <Erro:HAL.IPv4Mc.Error> MSM-B: SM failed to add 2:48 to IPMC 0, rv=-1 11/21/2012 16:59:53.70	Problem was fixed in ExtremeXOS 15.3 before it was released.

Table 4: Erroneously Listed Issues in the Open Table of ExtremeXOS 15.3

ID Number	Description	Reason Issues Was Removed
PD4-3159542451	For Summit X670v-48x series switches, ports with a SFP+_SR (SOURCEPHOTONICS) optic inserted with link up will flap if any other ports (two or more) are disabled/enabled. This issue does not occur with ExtremeXOS v15_1_2_12.	Cannot reproduce this problem.
PD4-3296418447	Router does not allow re-enabling OSPF/OSPFv3 routes into BGP. The following error message appears: “Error: Cannot change export policy for protocol ospf while export is enabled” You need to reboot the switch after issuing the command enable bgp export ospf ipv4-unicast to make this configuration.	Problem was fixed in ExtremeXOS 15.3 before it was released.
PD4-2897496481 PD4-2972980627 PD4-2918099300 PD4-2925483199	In BGP, various processes end unexpectedly and switches fail occasionally under certain remote switch rebooting and/or disabling peers conditions.	Cannot reproduce this problem.

Known Behaviors

The following are limitations in ExtremeXOS system architecture that have yet to be resolved.

Table 5: Known Behaviors, Platform-Specific and Feature Issues

ID Number	Description
General	
PD4-3734904546	sa-cache entry check failed for below scenarios: • Originate SA cache (with FHR and RP are the same) • Originate SA cache only if we are RP (or RP = FHR = DR) • Originate SA cache only if we are PMBR and RP and FHR
PD4-3317546201	Two issues in MAC-VLAN Mode: • Multicast cache entry for IGMP/MLD group is not deleted from hardware even after adding matching static FDB entry onto a different port in the same VLAN. • Multicast cache entry for IGMP/MLD group is not created in hardware after deleting matching FDB entry. **Workaround:** 1 Issue command: `clear igmp|mld snooping vlan <vlan_name>` [vlanname on which the fdbentry is created or deleted]. This command flushes the entire vlan. 2 Issue the command: `debug mcmgr clear <grp_Ip> <src_Ip> <vlan_name>` [User has to know the src_Ip and grp_Ip on which the cache is created].
PD4-3348898271	The static DHCP binding is not saved in the configuration, so saving, and then rebooting, loses the binding.
PD4-3109929170	After removing the zone, the debug command still displays the policy as NwZonePolicy. The mapping should be corrected to the policy itself as the zone is removed.
PD4-468366251	A network login client is not authenticated if the username is 32 characters. Only 31 character user names are supported, even if the user can create a 32-character username.
PD4-3315488109	After VLAN tag is modified on PMBR, traffic is not forwarded through dense circuit. **Workaround:** Enable MLD snooping on all interfaces.
PD4-3251586520	The IGMP groups are not deleted from the MVR VLAN when leave packets are sent in the edge VLAN. **Workaround:** Enable proxy when MVR is configured.
PD4-3352005341	Ping from ESRP master switch to host connected to ESRP slave (connected via host attach port) fails when the switch to which the host is connected is master for another ESRP domain.
PD4-3206377171	After a policy attached as a MVR static address range is modified, the ports for all MVR VLAN groups are deleted, while the addresses that are permitted by the policy are not deleted.

Table 5: Known Behaviors, Platform-Specific and Feature Issues (Continued)

ID Number	Description
PD4-3320002080	Sending vr-value as vr1 with vlan-tag from vm-map file with no user vr configured in the switch results in no vlan-tag and vr-name creation for that VM, and then creating user vr vr1 and running repository synch does not create vm with vlan-tag and vr vr1 as configured in vm-map files. **Workaround:** Restart process vmt and do run vmt repository synch.
PD4-3154851418	When both dynamic VLAN uplink port is configured and ISC port is configured dynamic VLAN created, add the uplink port as tagged, but the flag is only *11gV (should be with both "U" and "V" flag).
PD4-3269060537	The command `clear fdb` does not zero dropped counter in `show fdb` command.
PD4-3215358251	The help text (by pressing TAB) does not appear after issuing the command `configure vrrp vrrpvlan vrid 1 authentication none`.
PD4-3075918118	VM Statistics - Egress counter is not working.
PD4-3098599761	Changing from untagged to tagged traffic with the same VLAN tag does not add the ports as “tagged” and this results in traffic loss.
PD4-3080980181	When STP is configured and enabled the dynamic VLAN propagation suddenly vanishes.
PD4-3143967884	After authenticating two computers using the dot1x authentication method, a Remote Desktop session between two computers fails. **Workaround:** Enable computer-only authentication using the procedure from the Microsoft Windows knowledge base: http://support.microsoft.com/kb/929847.
PD4-2039102228	There is no CLI command to verify which control and protected VLANs belongs to which ERPS domains. Also missing are flags reserved for ERPS in `show vlan` command.
PD4-2744727326	`clear bgp` or `show bgp` commands should fail in VRF context.
PD4-2770013534	Valid MLD messages with unspecified address (::), are treated as valid MLD packets. instead, these should be silently dropped.
PD4-2770013437	MLD protocol Timer value is not inherited from the current querier's query message— instead it is always the configured value on this router.
PD4-2835155421	On a private VLAN [network VLAN] translated port, the packets egressing when captured, shows the subscriber VLAN tag instead of Network VLAN.
PD3-57182431	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.
PD4-1663984367	Whenever a (*, G) join is received, all hardware entries installed on non upstream (*, G) interfaces are cleared. Therefore, every 60 seconds, the L2 switching is affected, traffic comes to the CPU, and entries are re-learned.

Table 5: Known Behaviors, Platform-Specific and Feature Issues (Continued)

ID Number	Description
PD4-2110742669	When using SCP to transfer files to an Extreme switch, the transfer fails with an "incomplete command" error.
BlackDiamond Series Switches	
PD4-3652083671	On BlackDiamond 8800 series switches, the loopback port LED does not blink with mirroring enabled.
PD4-3305214940	On BlackDiamond X8 series switches, IGMP groups learned on an MLAG port are removed when the MLAG port goes down.
PD4-3266706442	The command `clear counters` followed by `show port congestion` results in an error if executed within about eight seconds of each other on BlackDiamond 8800 series switches.
PD4-3155474589	In BlackDiamond 8800 series switches, port flapping can occur when enabling mirroring instance with loopback port configured.
PD4-2938691821	For the BlackDiamond X8 series switches, differv value is not getting replace when dot1p examination is enabled on ingress port with diffserv replacement enabled for slow path l3 traffic.
PD4-2339271510, PD4-2180251961	For the BlackDiamond 8800 series switches, when running the `show tech` command on a backup MSM, an error message is displayed.
PD4-2854254274	For the BlackDiamond X8 and 8800 series switches, L3 traffic with IPv4 options or IPv6 ext. headers is not sent to the CPU when redirected by flow-redirection.
Summit Series Switches	
PD4-3314306502	On Summit X450a/e switches with XGM2-2bt modules, normal/ extended diagnostics fail.
PD4-3285450101	PIM signal 6 ends unexpectedly when disabling or enabling OSPF on Summit X670 stacks. Process PIM pid 1528 ends unexpectedly with signal 6.
PD4-3321289371	On Summit X460 series switches, flows are not removed when disconnected from controller.
PD4-3241288551	On Summit X440 series switches, IPv6 neighbor discovery is not happening to VRRP virtual IP in VRRPv3 MLAG setup.
PD4-3231034335	On Summit 80G stacks, JFFS2 warning messages occur while rebooting the 80G stack.
PD4-3332304721	On Summit X480 series switches, PIM process ends unexpectedly when executing `show pim ipv6` after creating multiple PIMv6-enabled VLANs.
PD4-3037333500	In Summit X670-48x series switches, only SFP+_SR (SOURCEPHOTONICS) ports are not coming up after restarting the port (25) and then save and reboot. This issue does not occur with Summit 650-24x and BlackDiamond 8800 series switches. **Workaround:** Disable, and then enable the far-end port.
PD4-3349524091	On Summit X460/X440 series switches, slot 2 reboots when more than the maximum permitted FDB entries are learned.

Table 5: Known Behaviors, Platform-Specific and Feature Issues (Continued)

ID Number	Description
PD4-2913932450	QSFP+LR (ColorChip) optics link is coming up when connected back-to-back and after a save and reboot of ExtremeXOS fails to detect the media type when a Q+LR4 in ports <port lists> on Summit X650 and X480-24x series switches. **Workaround:** Only the media type is getting properly set after unplug/plug the optics from ports. This issue is not seen with QSFP+ SR4 on Summit X650 and X480 series switches.
PD4-2760140871	For Summit X670 series switches, dynamically learned FDB entries on non-FIP snooping VLANs disappear after FIP snooping is disabled and re-enabled on the VLAN.
PD4-2835588361	For Summit X670 series switches, the `show conf bgp` command is not vr-aware. VR-default BGP config appears even though inside vrf-a context. It should show BGP config for vrf-a
PD4-2857038040	For Summit X650 series switches, differv value is not getting replace when dot1p examination is enabled on ingress port with diffserv replacement enabled for slow path l3 traffic.
PD4-2857038031	For Summit X650 series switches, dot1p value changes to zero when both dot1p and diffser examination is enabled on ingress port.
PD4-1637091230	With 4,000 VPWS sessions, traffic recovery takes approximately 8 minutes before a port flap occurs. **Workaround:** On a Summit X460, it is recommended that you only configure 1,000 VPWS instances.
E4G-200 and E4G-400 Cell Site Routers	
PD4-3316332889	ESVT fails to run even with just 10 ERPS rings configured in an E4G-200 cell site router node. ACL slice errors occur due to a hardware limitation.
PD4-3312009417	TDM UDP PWE fails to work when created between PE routers. TransmittedTDM packets are not received at the destination,
ACL	
PD4-2649674514	Policies with "redirect-port-list" as the action modifier do not get installed on a G48Te2 nor a 10G2Xc. It is not installed on either Summit X450a nor x450e.
PD4-2761666711	Redirect port list changes its behavior when sending slow path traffic.
PD4-1933402713, PD4-1933225935	The ACL action "copy-cpu-and-drop" is not copying EAPS control packets to the CPU.

Table 5: Known Behaviors, Platform-Specific and Feature Issues (Continued)

ID Number	Description
PD3-77983510	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 1,024 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 1,024 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 rules * 48 ports in the list <= 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.

Table 5: Known Behaviors, Platform-Specific and Feature Issues (Continued)

ID Number	Description
BGP	
PD4-2216087479	A confederation ID is used as an aggregator ID when in a confederation instead of an AS-number.
PD4-2125200453	A backup slot does not come up when rebooted with 1,000 non-unique routes on a Summit X480 stack.
IP Protocols	
PD4-3632921367	ECMP-PIM: Traffic recovers after up to 60 seconds when the route toward the source is withdrawn/re-advertised.
PD4-3564310831	ECMP-PIM: Up to two minutes of traffic loss occurs when ESRP slave switch transitions to master.
PD4-3512662174	IGMP Loopback-MVR: Invalid group version occurs when a static group is configured and an Ixia group expires.
PD4-3356887520	L2 data forwarding is not occurring after reconfiguring static MVR policy.
PD4-3302624090	The following error messages occur when disabling ports on an MLAG server node, which are connected to an MLAG peer, or when rebooting the server node: "11/29/2012 18:36:28.73 <Erro:IPMC.VSM.FndISCRecvrFail> MSM-A: ISC receiver not found for VLAN esrpv17, group 227.17.31.2, ISC 256:1" "11/29/2012 18:36:28.73 <Erro:IPMC.VSM.FndISCRecvrFail> MSM-A: ISC receiver not found for VLAN esrpv17, group 227.17.31.3, ISC 256:1"
PD4-3197436651	The display log message from the command `show ipstats` changed from "Router Interface on VLAN vlan1_2" to "Router Interface vlan1_2".
MPLS	
PD4-521915271	The Internet Group Management Protocol (IGMP) group reports may occasionally change from Version 2 to Version 3.
PD4-581950231	Multi-cast traffic is not received even though the rendezvous point (RP) tree and source information is shown in the PIM cache table
PD4-475414505	In more complex topologies, detour Label Switched Path (LSP) connections are not set up.
PD4-475414370	The following warning message is seen numerous times after changing VLAN Virtual Private LAN Services (VPLS) mappings: `<Warn:MPLS.LDP.InternalProb>`
PD4-464587012	All unicast traffic routed by MPLS is stopped when penultimate hop popping (PHP) is enabled on all MPLS VLANs. VPLS traffic is not impacted.

Table 5: Known Behaviors, Platform-Specific and Feature Issues (Continued)

ID Number	Description
PD3-203917264	If an LSP is already Up, and an ERO is added such that a subsequent path calculation will fail, the LSP will remain Up, and at the same time, continue to retry to calculate a new path with the new ERO. This situation is not clearly visible in the `show mpls rsvp-te lsp detail` output. The retry counters incrementing is really the only indication that this is happening. The fields showing the "`Msg Src`," "`Msg Time`," "`Error code`," and "`Error Value`" should be shown because the reason for the path calculation failure is shown in these fields.
PD3-93069318	Only VLANs configured as protocol *any* should be added to MPLS.
PD3-92653036	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.
PD3-157687121	ExtremeXOS software uses Control Channel Type 2 to indicate router alert label mode. In MPLS Router Alert Label mode, VCCV packets are encapsulated in a label stack. However, the existing VCCV packets are sent like a stack without any PW label.
PD3-104731701	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.
PD3-93630853	LDP should not advertise a label mapping for a direct VLAN that does not have IP forwarding enabled.
PD3-139423053	Running the `show mpls rsvp-te lsp summary` command on a system configured with 2,000 ingress LSPs takes an excessive amount of time to process.
PD3-111544904	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.
PD3-184989177	When an `LDP advertise static` setting is set to `all`, all static routes are treated as egress routes and egress LSPs are created. That is, a label is generated and advertised for the static route. If the router at the end of the static route advertises a label matching that static route, the LSP that was previously an egress LSP becomes a transit LSP. An ingress LSP should also be created whenever a label is received, however, the ingress LSP is never created. **Workaround:** Do not use the `LDP advertise static all` configuration in situations where an ingress LSP for a static route is required.
VLAN	
PD4-3134856251	The following error message appears when deleting dynamic VLANs: "mvrpLeaveCheck_cb: VID: 1003 not found. mvrpLeaveCheck_cb: VID: 1002 not found".

Resolved Issues in ExtremeXOS 15.3.5-Patch1-3

The following issues were resolved in ExtremeXOS 15.3.5-Patch1-3. ExtremeXOS 15.3.5-Patch1-3 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, ExtremeXOS 11.5.2.10, ExtremeXOS 11.6.5.3, ExtremeXOS 12.0.5, ExtremeXOS 12.1.7, ExtremeXOS 12.2.2-patch1-12, ExtremeXOS 12.3.6, ExtremeXOS 12.4.5, ExtremeXOS 12.5.5, ExtremeXOS 12.6.5.2-patch1-3, ExtremeXOS 12.7.1, ExtremeXOS 15.1.5.4-patch1-9, ExtremeXOS 15.2.4.5-patch1-5 ExtremeXOS 15.3.1.4-patch1-47 and ExtremeXOS 15.3.4.6.

Table 6: Resolved Issues, Platform-Specific and Feature Issues in ExtremeXOS 15.3.5-Patch1-3

ID Number	Description
General	
xos0056340	Unknown Layer 2 traffic from Isolated subscriber VLANs are forwarded to the remote MLAG ports, even though local MLAG ports are up.
xos0057211	Traffic gets forwarded for blackholed MAC address when limit learning is enabled.
xos0057463	The minimum key length supported when configuring an SSL certificate is 64 bits, which is considered medium strength and could be exploited by an attacker on the same physical network.
xos0057464	TLS protocol is impacted by CRIME (Compression Ratio Info-leak Made Easy) vulnerability.
xos0059655	Error appears when deleting static blackhole FDB entries.
xos0059730	The process mcmgr ends unexpectedly after removing a slot from existing SummitStack and unconfiguring that slot using the command `unconfigure slot slot_number`.
xos0059924	The output of the command `show access-list meter ports` displays additional meter name when only one meter is applied using ACL policy.
xos0061009	The output of the command `show netlogin MAC` output displays username for unauthenticated client.
xos0061178	Dynamic ACL for gratuitous ARP violation on LAG member ports are incorrectly getting installed on LAG master ports.
xos0061222	Gratuitous ARP packets for VRRP virtual IP addresses have ARP sender addresses as physical MAC addresses, instead of VRRP virtual MAC addresses.
xos0054075	Dynamic blackhole FDB entries persist after adding them as static non-blackhole FDB entries.
xos0055398	Authentication fails for a Netlogon client in dot1x mode, since the port added untagged in one VLAN cannot be moved to another VLAN.

Table 6: Resolved Issues, Platform-Specific and Feature Issues in ExtremeXOS 15.3.5-Patch1-3 (Continued)

ID Number	Description
xos0057045	Unable to match ARP packets using ACL match criteria "arp-sender-address" and "arp-target-address" in c-series I/O modules.
BlackDiamond 8800 Series Switches	
xos0054239	On BlackDiamond 8800 and BlackDiamond X8 series switches, slowpath forwarding of IPv4 packets can occur if there is contention for IP hardware table resources. The destination IP for slowpath forwarding can be for a local host for which there is a resolved ARP entry, but which was removed from the Layer 3 hardware table due to contention from IPv4 or IPv6 multicast or other unicast hosts. The destination IP for slowpath forwarding can also be for a remote host (a host reachable via a gateway), if all IPv4 LPM routes either do not fit in the LPM hardware table, or exceed the number of routes reserved using the command `configure iproute reserved-entries &ltnum_routes_needed&gt slot &ltslot&gt.`
BlackDiamond X8 Series Switches	
xos0059156	VRRP control packets are dropped due to congestion in tx queue under scaled environments.
BlackDiamond 8800 Series Switches	
xos0059671	On Summit X460 series switches with 750 W power supplies installed, log messages "`Power usage data unknown`" appear.

Resolved Issues in ExtremeXOS 15.3.5

The following issues were resolved in ExtremeXOS 15.3.5. ExtremeXOS 15.3.5 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, ExtremeXOS 11.5.2.10, ExtremeXOS 11.6.5.3, ExtremeXOS 12.0.5, ExtremeXOS 12.1.7, ExtremeXOS 12.2.2-patch1-12, ExtremeXOS 12.3.6, ExtremeXOS 12.4.5, ExtremeXOS 12.5.5, ExtremeXOS 12.6.5.2-patch1-3, ExtremeXOS 12.7.1, ExtremeXOS 15.1.5.4-patch1-9, ExtremeXOS 15.2.4.5-patch1-5 ExtremeXOS 15.3.1.4-patch1-47 and ExtremeXOS 15.3.4.6.

Table 7: Resolved Issues, Platform-Specific and Feature Issues in ExtremeXOS 15.3.5

ID Number	Description
General	
xos0053634	MAC-lockdown-timeout on user ports does not work as expected if Netlogin is enabled on those ports.
xos0053828	HAL process ends unexpectedly when all entries from network-zone are deleted and associated ACL is refreshed.
xos0053970	NTP process ends unexpectedly during switch reboot.
xos0054348	Cannot delete flow names after deleting, and then creating, the flow while the ACL is installed.
xos0056254	Management port remains in down state when peer switch has "auto-neg off" configuration. Issue occurs with Summit X460-G2, X670-G2, X450a, X450e, and BlackDiamond 8800 series switches.
xos0057407	Hops fields in DHCP packets are not incremented when processed by Bootprelay.
xos0058221	Rarely, OSPFv3 process ends unexpectedly with signal 11 when link flaps occur.
xos0060088	Kernel oops triggered rarely during continuous addition/deletion of ARP entries for long duration in presence of high CPU utilization.
Summit Series Switches	
xos0060142	When SummitStack master and backup slots experience prolonged loss of stacking communication (dual master issue), the backup becomes master and later fails due to HAL process ending unexpectedly.
BlackDiamond 8800 Series Switches	
xos0060301	Rarely, ports go into ready state when the connected devices are continuously auto-negotiating to different speeds. Disabling/enabling such port can trigger I/O module reboots.

Resolved Issues in ExtremeXOS 15.3.4-Patch1-14

The following issues were resolved in ExtremeXOS 15.3.4-patch1-14. ExtremeXOS 15.3.4-patch1-14 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, ExtremeXOS 11.5.2.10, ExtremeXOS 11.6.5.3, ExtremeXOS 12.0.5, ExtremeXOS 12.1.7, ExtremeXOS 12.2.2-patch1-12, ExtremeXOS 12.3.6, ExtremeXOS 12.4.5, ExtremeXOS 12.5.5, ExtremeXOS 12.6.5.2-patch1-3, ExtremeXOS 12.7.1, ExtremeXOS 15.1.5.4-patch1-9, ExtremeXOS 15.2.4.5-patch1-5 ExtremeXOS 15.3.1.4-patch1-47 and ExtremeXOS 15.3.4.6.

Table 8: Resolved Issues, Platform-Specific and Feature Issues in ExtremeXOS 15.3.4-Patch1-14

ID Number	Description
General	
xos0055795	The `show fdb stats vlan` command output does not show the number of MAC addresses learned over VPLS pseudowires.
xos0059077	Getting error after executing the `upload log` command multiple times.
xos0059789	Dos-Protect ACL is not cleared after continuous DOS attack occurs.
xos0059945	Memory corruption occurs rarely due to packet buffer overrun while sending/receiving control packets between slots.
xos0058391	Switches allow installing ACL policy with meter even though the corresponding meter is not yet created.
xos0059757	With per-VLAN IGMP snoop filter, backup VRRP does not forward hellos messages of the same VRIDs. This occurs only when the VRRP backup is master for a different VLAN using the same VRID and the IPMC traffic is being slow-path forwarded.
xos0060100	Kernel oops occurs due to memory corruption caused by slow-path forwarded traffic.
E4G-200 Cell Site Routers	
xos0058239	In E4G-200 cell site routers, power supply status displays incorrect value in the output of the `show power` command.
Summit X440 Series Switches	
xos0059500	On Summit X440 series switches with more than 1,500 IP ARP entries (exceeding supported hardware limit of ~400), and with ARP entries changing MAC address, some entries are not aged out of hardware. This can cause a mismatch between software and hardware when ARP is relearned with a different MAC address.
BlackDiamond 8800 Series Switches	
xos0059648	Static ARP entries are not properly synced with new Master Switch Fabric Module after failover.

Resolved Issues in ExtremeXOS 15.3.4-Patch1-13

The following issues were resolved in ExtremeXOS 15.3.4-patch1-13. ExtremeXOS 15.3.4-patch1-13 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, ExtremeXOS 11.5.2.10, ExtremeXOS 11.6.5.3, ExtremeXOS 12.0.5, ExtremeXOS 12.1.7, ExtremeXOS 12.2.2-patch1-12, ExtremeXOS 12.3.6, ExtremeXOS 12.4.5, ExtremeXOS 12.5.5, ExtremeXOS 12.6.5.2-patch1-3, ExtremeXOS 12.7.1, ExtremeXOS 15.1.5.4-patch1-8, ExtremeXOS 15.2.4.5-patch1-5 ExtremeXOS 15.3.1.4-patch1-47 and ExtremeXOS 15.3.4.6.

Table 9: Resolved Issues, Platform-Specific and Feature Issues in ExtremeXOS 15.3.4-Patch1-13

ID Number	Description
General	
xos0056323	On failed stack nodes, running any show commands produces an error.
xos0059243	The process `exsh` ends unexpectedly after executing a show command with a port list followed by invalid letters (for example, `show port 1:1,1:2ab`), and then pressing **TAB**.
xos0059661	Running extended diagnostics on backup MSM (Master Switch Fabric Module) can, under certain rare conditions, cause the `cfmgr` process to end unexpectedly on the master MSM.
xos0056342	Misleading power supply unit (PSU) traps are sent when PSUs are inserted or powered on/off.
BlackDiamond 8800 Series Switches	
xos0059605	Sys-health-check output shows false fabric port flap events between Master Switch Fabric Module (MSM) and I/O module.
BlackDiamond X8 Series Switches	
xos0055433	The tDiag process occasionally ends unexpectedly after executing `show debug system-dump MM B from MM-A`, when MM-B does not contain system dump.
Summit Family Switches	
xos0059447	Can use Python scripts to access debug shell and execute commands even though debug mode is not enabled making switches vulnerable to unauthorized use.
Summit X430 Series Switches	
xos0059524	Link status is incorrect when auto-polarity setting is off.

Resolved Issues in ExtremeXOS 15.3.4-Patch1-10

The following issues were resolved in ExtremeXOS 15.3.4-patch1-10. ExtremeXOS 15.3.4-patch1-10 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, ExtremeXOS 11.5.2.10, ExtremeXOS 11.6.5.3, ExtremeXOS 12.0.5, ExtremeXOS 12.1.7, ExtremeXOS 12.2.2-patch1-12, ExtremeXOS 12.3.6, ExtremeXOS 12.4.5, ExtremeXOS 12.5.5, ExtremeXOS 12.6.5.2-patch1-3, ExtremeXOS 12.7.1, ExtremeXOS 15.1.5.4-patch1-8, ExtremeXOS 15.2.4.5-patch1-5 ExtremeXOS 15.3.1.4-patch1-44 and ExtremeXOS 15.3.4.6.

Table 10: Resolved Issues, Platform-Specific and Feature Issues in ExtremeXOS 15.3.4-Patch1-10

ID Number	Description
General	
xos0054949	With VLAN aggregation, local multi-cast packets received on one sub-VLAN are flooded to other sub-VLANs.
xos0056994	Unable to add EAPS shared ports to VLANs even after disassociating them from VPLS domains.
xos0057435	Packets are dropped when learning is disabled in a VLAN when its associated ports are configured with limit learning in another VLAN.
xos0057785	STP domain tag is removed when all ports are deleted from STP auto-bind enabled-VLANs.
xos0058849	Jumbo frames are fragmented on LAG ports after re-configuring port sharing even though jumbo frame is enabled on those ports.
xos0058968	Error log "`Function Pointer Database is not fully initialized`" appears during bootup on non-Summit platforms.
xos0059002	Checkpoint errors occur during execution of STP debug command if switch contains many STP-enabled VLANs.
xos0059037	Pre-emphasis `show` command displays incorrect values for non-Summit X460 series switches' slots in mixed stacks.
xos0058801	IPv4 ECMP route entries learned by a routing protocol are sometimes removed from hardware when one of the next hop gateways goes down, but other gateways remain up.
xos0059222	SFLOW-sampled packets are flooded out of VLANs when these same packets are software learned.
xos0059305	OSPF consumes a large amount of memory when a large number of Link State Acknowledgment packets are queued up for transmission.
BlackDiamond X8 Series Switches	
xos0057352	Kernel crash occurs when there is a Layer 2 loop in the network.

Table 10: Resolved Issues, Platform-Specific and Feature Issues in ExtremeXOS 15.3.4-Patch1-10 (Continued)

ID Number	Description
Summit X440 Series Switches	
xos0058068	Summit X440-24tDC switches report maximum temperature limit 60°C under normal conditions
xos0058300	Packets are dropped on combo ports when the preferred medium is configured as copper force.
Summit X460 Series Switches	
xos0059131	Debounce timer is not getting configured if stack ports reside in different units. Also, pre-emphasis configuration should be rejected in alternate stacking mode.

Resolved Issues in ExtremeXOS 15.3.4-Patch1-8

The following issues were resolved in ExtremeXOS 15.3.4-patch1-8. ExtremeXOS 15.3.4-patch1-8 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, ExtremeXOS 11.5.2.10, ExtremeXOS 11.6.5.3, ExtremeXOS 12.0.5, ExtremeXOS 12.1.7, ExtremeXOS 12.2.2-patch1-12, ExtremeXOS 12.3.6, ExtremeXOS 12.4.5, ExtremeXOS 12.5.5, ExtremeXOS 12.6.5.2-patch1-3, ExtremeXOS 12.7.1, ExtremeXOS 15.1.5.4-patch1-8, ExtremeXOS 15.2.4.5-patch1-5 and ExtremeXOS 15.3.1.4-patch1-44.

Table 11: Resolved Issues, Platform-Specific and Feature Issues in ExtremeXOS 15.3.4-Patch1-8

ID Number	Description
General	
xos0052911	Client MAC address appears in switch's log message instead of DHCP server MAC address after configuring dhcp-snooping violation block-mac permanently.
xos0055347	Temperature reported in log messages is different than the output of the `show temperature` command.
xos0056423	The command `show access-list meter port` does not display the meters applied on the port via policy.
xos0057328	ACL rule to match IPv6 packets with arbitrary mask is not working as expected.
xos0057647	Packets are forwarded to CPU after deleting the VLAN with disable learning.
xos0057672	The process rtmgr ends unexpectedly when disabling GRE tunnels.
xos0058464	In ERPS rings, blocking the control channel by deleting the ports from the control VLAN causes a short loop in the ring.

Table 11: Resolved Issues, Platform-Specific and Feature Issues in ExtremeXOS 15.3.4-Patch1-8 (Continued)

ID Number	Description
xos0058695	Process emsServer ends unexpectedly with signal 6 when multiple VRRP messages are logged.
xos0054199	Ingress traffic stalls on port when switches receive continuous 802.3x pause frames on egress ports for that traffic stream.
xos0057179	ESRP feature is not enabled immediately after the installing an Advance Edge license.
SummitStack	
xos0054851	Show log and show license information does not appear in Summit standby slots.
xos0057255	Multi-cast entries are not programmed in hardware intermittently for certain multi-cast groups in stacking setup.
xos0057562	PoE initialization fails on certain SummitStack nodes with SSH enabled.
xos0058218	Need commands to tune debounce timer for stacking port.
Summit X430 Series Switches	
xos0052990	Summit X430 series switches do not retain configuration after rebooting.
Summit X440 Series Switches	
xos0058301	In Summit X440 series switches, error message "`mounting /dev/hda4 on /data failed`" appears during bootup.
Summit X460 Series Switches	
xos0058217	Need commands to tune pre-emphasis settings for stacking ports.
BlackDiamond 8800 Series Switches	
xos0053655	Running extended diagnostics on several I/O modules produces error messages and the diagnostics fail.
BlackDiamond X8 Switches	
xos0058568	Some front panel ports cannot be enabled after rebooting the I/O module.

Resolved Issues in ExtremeXOS 15.3.4-Patch1-5

The following issues were resolved in ExtremeXOS 15.3.4-patch1-5. ExtremeXOS 15.3.4-patch1-5 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, ExtremeXOS 11.5.2.10, ExtremeXOS 11.6.5.3, ExtremeXOS 12.0.5, ExtremeXOS 12.1.7, ExtremeXOS 12.2.2-patch1-12, ExtremeXOS 12.3.6, ExtremeXOS 12.4.5, ExtremeXOS 12.5.5, ExtremeXOS 12.6.5.2-patch1-3, ExtremeXOS 12.7.1, ExtremeXOS 15.1.5.4-patch1-8, ExtremeXOS 15.2.4.5-patch1-5, ExtremeXOS 15.3.1.4-patch1-44. For information about those fixes, see the release notes for the specific release.

Table 12: Resolved Issues, Platform-Specific and Feature Issues in ExtremeXOS 15.3.4-Patch1-5

ID Number	Description
General	
xos0047180	EMS process ends unexpectedly when a large quantity of logs are targeted to the console.
xos0051642	In MPLS-enabled switches, IP ARP is not getting resolved after executing `clear iparp` command.
xos0054825	Error message "Dropped CM_MSG_EXEC: Length 356 Peer 59 (snmpSubagent)" appears in log after switch reboots.
xos0056977	Client authenticated using netlogin dot1x gets incorrect IP address due to delay in moving port to success VLAN.
xos0056995	IPv6 traffic for routes with mask length >64 are not forwarded after clearing FDB
xos0057013	IPv6 traffic for routes with mask lengths greater than 64 characters is slowpath forwarded if switch has tunnels configured or when destination MAC address of the IPv6 packet is a virtual MAC address.
xos0057043	With MLAG and PVLAN configured, after disabling MLAG port, IP ARP entries continue to point to disabled MLAG port, instead of ISC port, causing traffic loss.
xos0057088	Cannot log on using SSH with a 32-character or greater password. After eight logon attempts, no more SSH connections are permitted.
xos0057578	The process snmpMaster ends unexpectedly on switches managed by Network Management tool when SNMP Informs are generated continuously.
xos0054940	SNMP requests should be forwarded to back-end client when configuration load or configuration save operation is in progress.
xos0053970	NTP process ends unexpectedly during switch reboot.
xos0057384	Hardware learning is not enabled on the sharing member ports after deleting an MLAG peer.

Table 12: Resolved Issues, Platform-Specific and Feature Issues in ExtremeXOS 15.3.4-Patch1-5 (Continued)

ID Number	Description
xos0057217	When both MLAG peers are turned off, and then only one MLAG peer is turned back on, MLAG ports in that switch are in the blocked state.
Summit X460 Series Switches	
xos0057024	Remote ports connected to 10G ports from XGM3 module experience link flap, and stacking link formed using ports from XGM3 module experience link flap.
xos0057916	Default debounce timer should be set to zero on stacking ports.
BlackDiamond 8800 Series Switches	
xos0057561	Enabling mirroring on BlackDiamond 8800 series switches with MSM-48c cause VRRP/LACP flapping.

Resolved Issues in ExtremeXOS 15.3.4

The following issues were resolved in ExtremeXOS 15.3.4. ExtremeXOS 15.3.4 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, ExtremeXOS 11.5.2.10, ExtremeXOS 11.6.5.3, ExtremeXOS 12.0.5, ExtremeXOS 12.1.7, ExtremeXOS 12.2.2-patch1-12, ExtremeXOS 12.3.6, ExtremeXOS 12.4.5, ExtremeXOS 12.5.5, ExtremeXOS 12.6.3, ExtremeXOS 12.7.1, ExtremeXOS 15.1.3, ExtremeXOS 15.2.2, ExtremeXOS 15.3.1, ExtremeXOS 15.3.2, and ExtremeXOS 15.3.3. For information about those fixes, see the release notes for the specific release.

Table 13: Resolved Issues, Platform-Specific and Feature Issues in ExtremeXOS 15.3.4

ID Number	Description
General	
xos0056048	CPU utilization is falsely reported as to high (99%) for OSPF process during graceful restart.
xos0052537	BFD process ends unexpectedly when deleting user-created virtual router.
xos0054573	L2 traffic is not flooded to network and subscriber VLAN ports after restarting process vsm.
xos0054109	FDB entries learned on MLAG ports are never aged out if the ports support hardware aging.
xos0057144	OSPF process ends unexpectedly during removal of OSPF neighbor configurations.
xos0054087	VPLS tunnel does not pass traffic when the tunnel port is part of a translation VLAN.

Table 13: Resolved Issues, Platform-Specific and Feature Issues in ExtremeXOS 15.3.4 (Continued)

ID Number	Description
xos0053857	LACP process ends unexpectedly in rare circumstances when enabling sharing on ports with active traffic flowing through them.
xos0053543	Switch responds to a GARP attack for an IP address that is configured as a static IP ARP entry with the switch MAC address when it should provide the MAC address listed in the static IP ARP entry.
xos0054097	Intermittently, MLAG local link state remains in ready state after restarting VSM process.
xos0055585	Multi-cast traffic takes up to 60 seconds to recover when an ingress port on a first hop router (FHR) is disabled.

xos0055593	With IP ARP distributed mode turned on, a few traffic streams are slowpath forwarded and the following error messages appear:
	`<Info:Kern.IPv4FIB.Info> Slot-9: dest 0x08021900 / 24 nexthop 0x0F14050F: DEFIP del: Hardware delete failed Invalid parameter (-4), multipath #installed=2, #ref=2`
	`<Warn:Kern.IPv4FIB.Warning> Slot-9: dest 0x08021900 / 24 nexthop 0x0F14040F: Unable to add route to unit 0, rc Entry exists. Shadow problem.`

xos0055611	PIM does not failover to alternate source received from the MSDP peers when the primary source fails.
xos0055659	The state-attribute value in RADIUS access challenge is truncated if its size is greater than 64 characters.
xos0055685	UPM process ends unexpectedly when the command `show config upm` is executed repeatedly for a prolonged time.
xos0056022	Topology change in ERPS sub-rings are not notified to the ERPS/EAPS main ring.
xos0056109	Traffic loss occurs for 15–30 seconds, when PIM non-DR changes to DR.
xos0050905	The following error appears while deleting the member port from sharing group on ISC ports: `"<Crit:vlan.err.fileIOCTL> System call ioctl failed: informCfgVlanRemPorts and 8 <Erro:Kern.Error> exvlan: configVlanRemovePort:2432: KERNEL_EXVLAN_ERROR: Failed to find vpif"`
xos0055374	Switch stops responding with kernel oops when issuing the command `configure iparp max_pending_entries` with a value less than the current max_pending_entries value.
xos0053748, xos0056992	The snmpMaster process ends unexpectedly when snmpMaster is restarted after changing engine-id.
xos0057159	ACL process ends unexpectedly when deleting access-list network zone.
xos0054208	HTTPs stops responding to netlogin requests after multiple refreshes of the customized logon page.

Table 13: Resolved Issues, Platform-Specific and Feature Issues in ExtremeXOS 15.3.4 (Continued)

ID Number	Description
xos0054525	The error "`adj 0.0.0.0: # L3 hash table entries already 0`" appears when the IPMC FDB table is cleared with a greater number of IPMC entries in the Summit X440 switch.
xos0056054	Disabling user-created mirror instance with ACL filter fails when a default mirror instance is enabled with ACL filter.
xos0055627	EDP process ends unexpectedly when a malformed packet has greater than 200-character length VLAN information in it.
xos0055783	Switches drop packets and display "`Invalid MAC Binding`" error when you remove an existing client and connect a different client with the same IP address.
xos0055939	EXSH assert failure occurs when executing commands containing port lists separated by commas when last port number is followed by TAB key sequence.
xos0056339	FDB learning does not occur after deleting/adding subscriber VLAN from PVLAN.
xos0056364	On BlackDiamond X8 and 8800 series switches, with distributed ARP turned on, L3 traffic doesn't egress after a link failover, even though ARP entries have been learned and they are pointing to the correct ports. The traffic starts flowing after executing the command `clear iparp`.
xos0057234	SNMP Informs are not being sent when there are unsent informs remaining in the queue.
xos0057264	Informs are not sent when there is only inform receiver configured on the switch.
xos0057281	Retries and new informs are not sent to non-responding inform receivers.
xos0057321	EDP process ends unexpectedly during switch reboot when VLAN name has 32 or greater characters.
xos0057538	OSPFv3 fails to select the best cost external route.
BlackDiamond 8800 Series Switches	
xos0057354	Kernel gets stuck after issuing the command `clear fdb`, followed by MSM failover when switch has highly scaled FDB and ARP entries.
BlackDiamond X8 Series Switches	
xos0056292	BlackDiamond X8 series switches reboot due to Kernel oops due to memory corruption.
Summit Family Switches	
xos0057047	On Summit X460 series switches and E4G-200 cell site routers, ports with BASE-T optics are not coming up.
Summit X460 Series Switches	
xos0055217	On Summit X460 stacks, EDP does not work in XGM3SB-4sf VIM modules.
xos0055416	On Summit X460 series switches, after enabling jumbo frames on 10G ports on XGM modules, doing either a save and reboot or changing port speed settings removes the jumbo frames setting.

Table 13: Resolved Issues, Platform-Specific and Feature Issues in ExtremeXOS 15.3.4 (Continued)

ID Number	Description
Summit X450 Series Switches	
xos0057375	Multi-cast cache entries for local mcast group (for example, 224.0.0.x/24) go out of sync between hardware units and software.
Summit X670 Series Switches	
xos0055074	On Summit X670v-48x series switches, links go down after rebooting if the ports are configured with auto negotiation off and the speed is 1G on both peers when using a mini Gigabit interface converter.
SummitStack	
xos0057214	The rtmgr process ends unexpectedly in backup node when deleting port from VLANs.

Resolved Issues in ExtremeXOS 15.3.3-Patch1-10

The following issues were resolved in ExtremeXOS 15.3.3-patch1-10 ExtremeXOS 15.3.3-patch1-10 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, ExtremeXOS 11.5.2.10, ExtremeXOS 11.6.5.3, ExtremeXOS 12.0.5, ExtremeXOS 12.1.7, ExtremeXOS 12.2.2-patch1-12, ExtremeXOS 12.3.6, ExtremeXOS 12.4.5, ExtremeXOS 12.5.5, ExtremeXOS 12.6.3, ExtremeXOS 12.7.1, ExtremeXOS 15.1.3, ExtremeXOS 15.2.2, ExtremeXOS 15.3.1, ExtremeXOS 15.3.2, and ExtremeXOS 15.3.3. For information about those fixes, see the release notes for the specific release.

Table 14: Resolved Issues, Platform-Specific and Feature Issues in ExtremeXOS 15.3.3-Patch1-10

ID Number	Description
General	
PD4-4600284820	Login authentication events occur for Lawful Intercept users if they are logged in using SSH.
PD4-4570039892	Lawful intercept users can log on with a case-insensitive account name, but changing passwords is not permitted.
PD4-4388036495	OSPFv3 external routes are not added back into the routing table after a topology change in the network.
PD4-4388036893	VRRP trackip-route feature fails to detect invalid routes when they are configured across multiple VRRP instances.
PD4-4552209254	Unsupported SNMP MIB "extremeTrapDiagPortDiagnostics" should be removed from the ExtremeXOS MIB file.
PD4-4388036781	OSPFv3 BFD session goes down after changing router-id.

Table 14: Resolved Issues, Platform-Specific and Feature Issues in ExtremeXOS 15.3.3-Patch1-10 (Continued)

ID Number	Description
PD4-4388036984	OSPFv3: Import policy changing the cost for matched routes does not take effect until after disabling, and then enabling OSPFv3.
PD4-4388037081	The output of the `show vrrp` command is zero for the VRRP advertisement interval if the configured value is below one second.
PD4-4388078784	Process netTools ends unexpectedly with signal 6 while doing SNMP walk on IPv6 prefix table.
PD4-4387722582	The VRRP maximum scaling limit is 511, but you can create 512 instances, and you do not get an error until you create 513 instances.
PD4-4388078226	OSPFv3 process ends unexpectedly after switch reboot or when OSPFv3 is disabled.
PD4-4388078289	OSPFv3: After configuring virtual link, external routes are not learned properly in a transit switch through which the virtual link is established.
PD4-4551909669	In STP domain, deleting a port from carrier VLAN is working, but re-adding a port is not successful if the same port is part of another protected VLAN.
PD4-4387722900	OSPFv3 LSAs are discarded for certain prefixes when the number of prefixes is at least 16.
PD4-4446649731	CliMaster ends unexpectedly with signal 6 when a telnet session loses connectivity to the switch during a lengthy command execution.
PD4-4388036384	VRRPv3 cannot be enabled until both virtual IPv6 addresses and virtual link-local IPv6 addresses are configured.
PD4-4388036615	VRRPv3: Switch does not send unsolicited neighbor advertisement packets when transitioning from VRRP backup to VRRP master.
PD4-4611406371	By enabling ACL log filters, admin users can see the dynamic ACL binding/unbinding information of Lawful Intercept users
PD4-4387723108	Router does not re-advertise OSPFv3 routes with new link-local addresses when link-local addresses change.
PD4-4388078463	Disabling/enabling ports in OSPFv3-enabled VLANs results occasionally in error messages like the following: `<Warn:ospfv3.pkt.DscrdLSAPfxLenInv> MM-B: [OSPF-Default] Discarded LSA Area(0.0.0.0):Type(0x2009):0.0.0.1:1.1.1.111 received with invalid prefix length of -1 bits from neighbor 1.1.1.111 on vlan LAgg1_LAgg2`
PD4-4388078508	The following error message appears when a port is brought up, even though switch does not have OSPFv3 configuration: `<Erro:cm.sys.actionErr> Error while loading "ospf6Global": ERROR: Interface Cost is inconsistent with Bandwidth of the interfaces."`
PD4-4615122663	OSPFv3 process ends unexpectedly with signal 6 during failover in switch with multiple virtual links.

Table 14: Resolved Issues, Platform-Specific and Feature Issues in ExtremeXOS 15.3.3-Patch1-10 (Continued)

ID Number	Description
PD4-4615129603	Unable to delete OSPFv3 areas, even though there aren't any OSPFv3 interfaces in that area.
PD4-4573804222	If Lawful Intercept users create ACLs with no match conditions, corresponding log messages appear in admin session.
PD4-4615129783	Deleting an OSPFv3 interface from the backbone area and adding the same interface to new area fails.
PD4-4604816163	OSPFv3 is not selecting highest area ID while forwarding traffic to ASBR.
PD4-4481256571	After multiple reboots, VRRP instances stay in INIT state when ELSM and VRRP are running over the same single port.
PD4-4573728051	If Lawful Intercept users create a dynamic ACLs and apply them on wildcard, this appears in the output of the command `show access-list any` of admin session.
PD4-4570291762	When there is a delay triggering a cyclic UPM profile, the next FireTime is calculated using the delayed current time.
PD4-4552209406	Executing the command `show port transceiver information` causes memory leaks in kernel.
PD4-4615065418	Changing instance ID along with timer causes OSPFv3 neighborship to go down.
PD4-4612108362	HAL process ends unexpectedly when unconfiguring clear-flow access-list containing mirror actions.
PD4-4429113480	Disabling jumbo frame causes additional ACL rules to be used.
PD4-4367450551	In the output of the command `show ospfv3 interface vlan <vlan_name>`, the instance-id does not reset to default value 0 even after deleting the VLAN from OSPFv3.
PD4-4630299803	NTP process ends unexpectedly while executing the command `show ntp association`.
PD4-4629644058	ACL rules with match condition igmp-msg-type do not work when packets contain ip-option.
PD4-4623200646	In Summit, BlackDiamond 8800, and BlackDiamond X8 platforms, need a mechanism to handle local multicast packets destined to 224.0.0.x group to get flooded in hardware.
PD4-4431944998	The output of the command `debug hal show congestion` displays incorrect CPU congestion counter values that are much higher than the actual number of dropped packets.
PD4-4387722973	OSPFv3 sessions stays in exstart/exchange state when switch has 64 OSPFv3 neighbors.
Summit X480 Series Switches	
PD4-4429516111	On Summit X480 series switches in 80G stack mode, the stack port counters are not incrementing correctly.

Table 14: Resolved Issues, Platform-Specific and Feature Issues in ExtremeXOS 15.3.3-Patch1-10 (Continued)

ID Number	Description
BlackDiamond 8800 Series Switches	
PD4-4388078392	Memory depletion occurs in BlackDiamond 8900 XL series I/O modules with 100 OSPFv3 neighbors.
PD4-4621469395	In BlackDiamond 8900 switches with 8900-10G24X-c modules, the following error message appears after executing the command `show tech` or `debug hal show version slot <slot#>` from MSM-B: `<Erro:Kern.Error> MSM-B: ahd_adm1066_cmd: Error reading ADM1066 for slot 9 rc=-1`
PD4-4421929616	"`Could not derive slot/port from modid/port`" error message appears while doing MSM failover with VPLS traffic.
PD4-4388036668	OSPFv3 ends unexpectedly with signal 11 after reseting the I/O module followed by a manual MSM failover.
PD4-4388036287	When deleting VRRP instances, the switch does not send a final VRRP advertisement with priority zero.

Resolved Issues in ExtremeXOS 15.3.3-Patch1-9

The following issues were resolved in ExtremeXOS 15.3.3-patch1-9 ExtremeXOS 15.3.3-patch1-9 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, ExtremeXOS 11.5.2.10, ExtremeXOS 11.6.5.3, ExtremeXOS 12.0.5, ExtremeXOS 12.1.7, ExtremeXOS 12.2.2-patch1-12, ExtremeXOS 12.3.6, ExtremeXOS 12.4.5, ExtremeXOS 12.5.5, ExtremeXOS 12.6.3, ExtremeXOS 12.7.1, ExtremeXOS 15.1.3, ExtremeXOS 15.2.2, ExtremeXOS 15.3.1, ExtremeXOS 15.3.2, and ExtremeXOS 15.3.3. For information about those fixes, see the release notes for the specific release.

Table 15: Resolved Issues, Platform-Specific and Feature Issues in ExtremeXOS 15.3.3-Patch1-9

ID Number	Description
General	
PD4-4550524998	FDB entries are not learned using VPLS when switch is in software learning mode
PD4-4583322981	Inappropriate upgrade messages appear when changing firmware to a supported version.
PD4-4552704871	In BlackDiamond X8 and 8800 series switches, with distributed ARP turned on, L3 traffic doesn't egress after a link failover, even though ARP is learned correctly and is pointing to the correct port. The traffic starts flowing after executing the command `clear iparp`.

Table 15: Resolved Issues, Platform-Specific and Feature Issues in ExtremeXOS 15.3.3-Patch1-9 (Continued)

ID Number	Description
PD4-4195170819	Switch fails to recognize previously learned MAC addresses when configuring the features “MAC Lockdown” and “Limit Learning”.
PD4-4308318281	Error message occur while doing snmpwalk for `PimIpMRouteEntry` object.
PD4-4402508041	IPFIX tags 152(flowStartMilliseconds) and 153(flowEndMilliseconds) should be added to the existing IPFIX template.
PD4-4552272553	STP and TRILL processes end unexpectedly while adding a member VLAN to the translation VLAN, when the translation VLAN name has 25 characters.
PD4-4468873921	With Option-82 enabled, DHCP request packets contain incomplete circuit-id information when the string exceeds 15 characters.
PD4-4489666943	BGP export policy with match condition "next-hop" does not work as expected.
PD4-4467744630	Enhance the output of the command `debug hal show sys-health-check` to include I/O module memory information and Async queue counters.
PD4-4495362758	The following error message appear if the command `show mpls statistics l2vpn` is executed immediately after the command `clear counters`: `"Error: MPLS statistics database is not defined"`
PD4-4536545874	DHCP decline packets are dropped if the client address field within the DHCP decline packet is 0.0.0.0.
PD4-4267672393	ACL error message `"Failed to install dynmic acl"` appears sometimes after rebooting or perfomring a failover of the switch with VLAN aggregation or IP security configuration.
PD4-4490184837	Traffic loss occurs in the switch due to parity errors in the L3 table.
PD4-4092434449	Creating BGP neighbors with a peer group configuration is not inheriting the outbound route-policy associated with the peer group.
Summit Family Series Switches	
PD4-4478417281	In SummitStacks, ports stop forwarding traffic when egress mirroring is configured on some other port.
Summit X430 Series Switches	
PD4-4587872519	Summit X430-24t and X430-48t series switches’ fans should not run at full speed until the temperature reaches 50°C.
Summit X460 Series Switches	
xos0052683	Stacking does not come up when trying to use one port in alternate and another port in native mode for stacking.
PD4-4521548810	In Summit X460-48t/X460-48p stacks, the default debounce timer (150 ms) on 10G ports of backup nodes may show a zero value after a stack reboot.

Table 15: Resolved Issues, Platform-Specific and Feature Issues in ExtremeXOS 15.3.3-Patch1-9 (Continued)

ID Number	Description
Summit X480 Series Switches	
PD4-4541155871	In Summit X480 series switches, some FDB entries become stale when a large number of FDB entries are learned as a batch from a port residing in the VIM4-40G4X module.
Summit X650 Series Switches	
PD4-4557266501	Unable to create LAG groups with custom algorithm in X650 SummitStacks.
Summit X670 Series Switches	
PD4-4446649817	In Summit X670v-48x series switches, ports with 10/100/1000BASE-T optics do not become active after multiple reboots.
BlackDiamond 8800 Series Switches	
PD4-4507887015	In BlackDiamond 8800 series switches, optimize the memory usage of I/O modules to provide more free memory after a bootup.

Resolved Issues in ExtremeXOS 15.3.3-Patch1-6

The following issues were resolved in ExtremeXOS 15.3.3-patch1-6 ExtremeXOS 15.3.3-patch1-6 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, ExtremeXOS 11.5.2.10, ExtremeXOS 11.6.5.3, ExtremeXOS 12.0.5, ExtremeXOS 12.1.7, ExtremeXOS 12.2.2-patch1-12, ExtremeXOS 12.3.6, ExtremeXOS 12.4.5, ExtremeXOS 12.5.5, ExtremeXOS 12.6.3, ExtremeXOS 12.7.1, ExtremeXOS 15.1.3, ExtremeXOS 15.2.2, ExtremeXOS 15.3.1, ExtremeXOS 15.3.2, and ExtremeXOS 15.3.3. For information about those fixes, see the release notes for the specific release.

Table 16: Resolved Issues, Platform-Specific and Feature Issues in ExtremeXOS 15.3.3-Patch1-6

ID Number	Description
General	
PD4-3992725987	Dynamic ACLs should have precedence over policy-based ACLs. However, after creating both ACL types, and then saving/ rebooting switch, policy-based ACLs have priority.
PD4-4470075281	MAC addresses are not re-learned for the incoming VPLS traffic after executing the command `clear fdb vpls`, but traffic flows to service VLAN ports correctly.
PD4-4399372681	The command `upload debug` produces error when the same policy is applied for SNMP and telnet as access-profiles.
PD4-4454790554	IPMC: Multi-cast cache creation can fail for reserved multi-cast addresses (for example, 224.0.0.x/8) on VLANs with IP addresses configured and 100+ active ports.
PD4-4408438667	ACL process ends unexpectedly when policies are removed from the identity-management role after unsuccessful ACL policy refresh events due to slice full condition.
PD4-4364775846	The help description for the command `show lacp member-port <port>` should show "port" instead of "port-list".
PD4-4485052499	ERPS status stays in idle state even when CFM detects port link down events.
PD4-3761737021	Routing tables do not update after resetting RIP neighborship when two RIP routers export the same routes to two different ASBRs.
PD4-4456297215	Log messages should appear when adding VLANs into an OSPF areas without deleting those VLANs from existing OSPF areas.
PD4-4362903645	Pinging produces the error message "Too many concurrent ping requests".
PD4-4280568717	When jumbo frames are enabled on some ports, LACP error "pibL3MTUExceededInstallFilterLag" appears after disabling sharing in one port, and then enable sharing on another port.
PD4-4399373411	Enabling static load sharing with custom algorithm produces the error message "Failed to configure the hash algorithm for load sharing group".

Table 16: Resolved Issues, Platform-Specific and Feature Issues in ExtremeXOS 15.3.3-Patch1-6 (Continued)

ID Number	Description
PD4-4447709745	Deleting untagged VMAN ports that are tagged ports on other VMANs produces the error "Jumbo still enabled".
PD4-4476658620	Ping doesn't work on VPLS VLANs across pseudo-wires.
PD4-4439432844	Quiting or exiting the BCM shell with at least one uppercase letter causes the bcm.shell thread to end.
PD4-3999409150	After creating/deleting 2,047 meters, you cannot create any more meters.
PD4-4380780041	Manually ending a session with a CLI command operation still in progress causes the cliMaster process to end unexpectedly with signal 11,
PD4-4456297129	Two loop conditions produces only one ELRP log message.
Summit Family Series Switches	
PD4-4481861582	Enabling MPLS license on standby slot causes process HALto end unexpectedly with signal 11.
PD4-4379703782	SNMP query on Summit stacks for extremeMemoryMonitorsystem does not return memory usage details of backup node.
Summit X430 Series Switches	
PD4-4439482748	MVR commands should be blocked on Summit X430 series switches, since the feature is not supported.
Summit X460 Series Switches	
PD4-4212233229	On Summit X460 series switches, 10G links flap frequently, but briefly, on either the Summit X460 side or at the peer switch side.
BlackDiamond 8800 Series Switches	
PD4-4421929581	Executing the command `show access-list usage acl-slice port <port number>` produces the error "Unable to connect to slot".

Resolved Issues in ExtremeXOS 15.3.3-Patch1-4

The following issues were resolved in ExtremeXOS 15.3.3-patch1-4 ExtremeXOS 15.3.3-patch1-4 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, ExtremeXOS 11.5.2.10, ExtremeXOS 11.6.5.3, ExtremeXOS 12.0.5, ExtremeXOS 12.1.7, ExtremeXOS 12.2.2-patch1-12, ExtremeXOS 12.3.6, ExtremeXOS 12.4.5, ExtremeXOS 12.5.5, ExtremeXOS 12.6.3, ExtremeXOS 12.7.1, ExtremeXOS 15.1.3, ExtremeXOS 15.2.2, ExtremeXOS 15.3.1, ExtremeXOS 15.3.2, and ExtremeXOS 15.3.3. For information about those fixes, see the release notes for the specific release.

Table 17: Resolved Issues, Platform-Specific and Feature Issues in ExtremeXOS 15.3.3-Patch1-4

ID Number	Description
General	
PD4-4034377698	OSPFv3 is sending IPv6 addresses instead of the prefix in the address prefix field of Link LSA, when the IPv6 address of a VLAN is configured with mask 97 and above.
PD4-4161632728	The error message: "Error: Failed to install image - mount: mounting /dev/mtdblock2 on /exos failed: Device or resource busy" appears when uninstalling SSH XMOD.
PD4-4271398579	Unable to disable/enable port using Screenplay.
PD4-4406011717	Restart process class OSPF does not work.
PD4-4370766841	AAA process ends unexpectedly on switches with TACACS authorization enabled when the TACACS accounting server is slow processing the CLI executed.
PD4-4349509481	VRRP MAC addresses are not programmed in hardware if corresponding hash bucket is already full with other normal MAC address entries.
PD4-4341426359	XMLD process ends unexpectedly with signal 6 when switches have 2,048 XML requests pending in the queue.
PD4-4286668455	VPLS not passing traffic for around one minute after disable/ enable VPLS VLAN.
PD4-4409195453	VPWS feature stops working while configuring MLAG.
PD4-4410100420	With `iproute mpls next-hop` configured, pinging a neighboring router loopback address fails when no source IP address is specified.
PD4-4409195355	OSPFv3 cost is missing while deleting/adding the VLAN from OSPFv3.
PD4-4406011595	ACL error messages "Failed to install dynmic acl vlanAggDHCP" appear when associating more than one sub-VLAN with a super-VLAN.
PD4-4387557269	The process mcmgr ends unexpectedly since the null pointer is not handled.
PD4-4402537380	Switch stops responding when restarting ESVT process.

Table 17: Resolved Issues, Platform-Specific and Feature Issues in ExtremeXOS 15.3.3-Patch1-4 (Continued)

ID Number	Description
PD4-4402537143	PVLAN with MLAG: Unable to ping network VLAN interface IP address from subscriber VLAN.
PD4-4405421722	Error message "OID not increasing" appears when performing SNMP walk for extremePortLoadshare2Table.
PD4-4402537255	User-defined mirror instance does not work if ACL with mirror rule is applied on VMAN/VLAN.
BlackDiamond 8800 Series Switches	
PD4-4406011523	DHCP binding restoration fails after rebooting BlackDiamond 8800 series switches with dual MSM.
PD4-4404955373	Packets are software forwarded after MSM failover followed by clearing the FDB.
PD4-4402537190	Warning message "canot disable ctrl" appears during bootup.
PD4-4404955305	Error messages appear when disabling/enabling learning on the port when VPLS is configured.
PD4-4402537320	Error messages appear when disabling/enabling I/O manually with port isolation configurations.
PD4-4368267887	In BlackDiamond 8800 series switches with MSM-B as the master, EPM process ends unexpectedly when SNMP query checks download image status.
PD4-4404955153	LAG ports are not added to the aggregation group after a MSM-failover followed by port restart.
PD4-4406011782	Some I/O modules go to failed state after issuing the command `disable/enable ports all`.
PD4-4405421820	Rarely, Kernel gets stuck when performing an MSM failover.
Summit X440 Series Switches	
PD4-4405737888	On Summit X440 series switches, data packets are dropped on the ports when ACL with dsap match condition is applied.
Summit X670 Series Switches	
PD4-4244923694	On Summit X670 series switches, link becomes active with BASET-SFP even though no cable is inserted.
PD4-4391249595	On X670v-48x SummitStacks, stack ports are getting stuck in "No-Neighbor" state while converting from v160G to v320G or vice versa.

Resolved Issues in ExtremeXOS 15.3.3-Patch1-3

The following issues were resolved in ExtremeXOS 15.3.3-patch1-3 ExtremeXOS 15.3.3-patch1-3 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, ExtremeXOS 11.5.2.10, ExtremeXOS 11.6.5.3, ExtremeXOS 12.0.5, ExtremeXOS 12.1.7, ExtremeXOS 12.2.2-patch1-12, ExtremeXOS 12.3.6, ExtremeXOS 12.4.5, ExtremeXOS 12.5.5, ExtremeXOS 12.6.3, ExtremeXOS 12.7.1, ExtremeXOS 15.1.3, ExtremeXOS 15.2.2, ExtremeXOS 15.3.1, ExtremeXOS 15.3.2, and ExtremeXOS 15.3.3. For information about those fixes, see the release notes for the specific release.

Table 18: Resolved Issues, Platform-Specific and Feature Issues in ExtremeXOS 15.3.3-Patch1-3

ID Number	Description
General	
PD4-4325909757	Disabling or enabling LAG ports produces error message: `"Failed to configure load sharing group 1 on slot 1 unit 0: Invalid identifier."`
Summit Family Switches	
PD4-4165846347	In SummitStacks, the following error message appears regarding the backup node when clearing IP multi-cast entries: `"<Warn:HAL.IPv4Adj.Warning> Slot-2: adj 0.0.0.0: # L3 hash table entries already 0."`
Summit X430 Series Switches	
PD4-4251722654	Unable to ping an IPv6 interface created on Summit X430 series switches.

Resolved Issues in ExtremeXOS 15.3.3-Patch1-2

The following issues were resolved in ExtremeXOS 15.3.3-patch1-2 ExtremeXOS 15.3.3-patch1-2 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, ExtremeXOS 11.5.2.10, ExtremeXOS 11.6.5.3, ExtremeXOS 12.0.5, ExtremeXOS 12.1.7, ExtremeXOS 12.2.2-patch1-12, ExtremeXOS 12.3.6, ExtremeXOS 12.4.5, ExtremeXOS 12.5.5, ExtremeXOS 12.6.3, ExtremeXOS 12.7.1, ExtremeXOS 15.1.3, ExtremeXOS 15.2.2, ExtremeXOS 15.3.1, ExtremeXOS 15.3.2, and ExtremeXOS 15.3.3. For information about those fixes, see the release notes for the specific release.

Table 19: Resolved Issues, Platform-Specific and Feature Issues in ExtremeXOS 15.3.3-Patch1-2

ID Number	Description
General	
PD4-3288465234	Log messages are not generated when SSH2 access is rejected by access-profile.
PD4-4280254748	ACL with match condition snap-8192, matches multi-cast traffic as well.
PD4-4265823545	Kernel error messages should provide additional debug information regarding the failure encountered.
PD4-4132061079	The process ospfv3 ends unexpectedly with signal 11 when unconfiguring and reconfiguring an IPv6 address on a loopback VLAN.
PD4-4146698455	Deleting a user-created virtual router causes the switch to become unresponsive when SNTP is enabled for that virtual router.
PD4-3803187216	Should not be able to create more than 2,048 meters.
PD4-4255242081	Configuring a dhcp-address-range for a management VLAN should not be allowed.
PD4-4234127320	NTP process ends unexpectedly with signal 6 when disabling an NTP-enabled VLAN.
PD4-4192807842	VRRPv2 dual master with sub-second advertisement Interval.
PD4-4108247631	Process SNMPMASTER ends unexpectedly with signal 11 when running continuous SNMPWALK on a switch.
PD4-4256008048	DoS protection in simulated mode logs added ACLs, but traffic is not blocked.
PD4-4175423951	VRRPv3: Switch is not sending unsolicited neighbor advertisement packet when it is transitioning from VRRP backup to VRRP master.
PD4-4258627391	When STP port priority is set to zero, the output of the command `show configuration stp` does not reflect the configured priority value zero.
PD4-4241121898	Switch is learning MAC addresses from the STP-blocked port if AVB is enabled.

Table 19: Resolved Issues, Platform-Specific and Feature Issues in ExtremeXOS 15.3.3-Patch1-2 (Continued)

ID Number	Description
PD4-4264557464	OSPF routes are cleared and not updated again when performing an MSM failover with OSPF graceful restart enabled along with MPLS RSVP-TE protocol.
PD4-4250686087	During switch bootup, some slots go to failed state when the configuration has dot1p examination, replacement, diffserv examination and replacement on all ports.
PD4-4250686171	After rebooting a switch with a private VLAN configuration, some slots go to failed state.
PD4-4255312476	Management port becomes unresponsive and stops transmitting traffic at random times if peer switch has auto-negotiation turned off.
PD4-4237751413	In Summit X460-24p switches, the following error messages appears when enabling and disabling load sharing: "Failed to configure load sharing group 2:1 on slot 1 unit 0: Entry not found"
Summit Family Switches	
PD4-403788199	Netlogin process ends unexpectedly when you log on through netlogin web-based authentication.
PD4-4245324652	Partial content of Summit 1GB compact flash is not erased during rescue.
PD4-4239458811	In SummitStacks, slots move to failed state after restarting VRRP process if VRRP is enabled on the network VLAN of PVLAN. After rebooting slot changes to operational state from failed state, and then VRRP process ends unexpectedly with signal 11.
PD4-4237751459	In SummitStacks, after `run failover` the LAG group configuration is removed from hardware, but the command `show port sharing` is still shows the LAG group.
PD4-4133539856	In SummitStack, VRRP MAC address is not checkpointed to other slots after those slots are rebooted.
Summit X670 Series Switches	
PD4-4247635290	In Summit X670v-48x SummitStacks, Kernel error message appears while enabling/disabling diffserv on all ports.
E4G-200 Cell Site Routers	
PD4-4175527148	Unable to create LAG groups on a port where ERPS was configured previously with CFM.
BlackDiamond X8 Series Switches	
PD4-4230894168	When VRRP master, BlackDiamond X8 series switches are not sending router-advertisement packets with VRRP virtual IP addresses.
BlackDiamond 8800 Series Switches	
PD4-4274870531	The following error appears sometimes when rebooting with SSH2 enabled: "Timeout occurred while retrieving information from hardware".

Resolved Issues in ExtremeXOS 15.3.3

The following issues were resolved in ExtremeXOS 15.3.3. ExtremeXOS 15.3.3 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, ExtremeXOS 11.5.2.10, ExtremeXOS 11.6.5.3, ExtremeXOS 12.0.5, ExtremeXOS 12.1.7, ExtremeXOS 12.2.2-patch1-12, ExtremeXOS 12.3.6, ExtremeXOS 12.4.5, ExtremeXOS 12.5.5, ExtremeXOS 12.6.3, ExtremeXOS 12.7.1, ExtremeXOS 15.1.3, ExtremeXOS 15.2.2, ExtremeXOS 15.3.1, and ExtremeXOS 15.3.2. For information about those fixes, see the release notes for the specific release.

Table 20: Resolved Issues, Platform-Specific and Feature Issues in ExtremeXOS 15.3.3

ID Number	Description
General	
PD4-4192808224	The access-list policy is not applied when using destination-zone attribute in the rule entry for the first time.
PD4-4219421276	Unable to create new VLAN via XML.
PD4-4195363389	ACL to permit a specific TCP port range does not work if the destination-zone attribute is present in the policy file.
PD4-4200853323	RSVP-TE LSP: traffic routed via LSP is not restored back via LSP after failure and recovery, but it is forwarded using OSPF.
PD4-4085086075	LLDP detect and undetect events are not properly triggered when netlogin,identity management and UPM are running on the same port.
PD4-4193425936	Rate-limit flood command is not blocking traffic if the value is set to 0 pps.
PD4-4210036237	Memory leak occurs after creating and deleting ACL network-zones with IP/MAC attributes.
PD4-4211093787	Memory leak occurs after configuring and unconfiguring ACL policies that have network-zones.
PD4-4186259011	ScreenPlay does not properly display details about ports and VLANs.
PD4-4195557010	STP ports from the STP domain are removed when you remove the untagged port from the VLAN that is auto-binded to an STP domain.
PD4-4213889961	ACL process signal 6 ends unexpectedly when refreshing zone policies.
PD4-4183786632	Process ipSecurity ends unexpectedly when 64-byte TCP/IP frames with flags TCP FIN, URG, and PSH bits are received.
PD4-4128868964	Some valid MLD packets are rejected by switch as error packets.
PD4-4178084731	Control packets are not egressing if switch is rebooted with `disable ports all` configuration, and then you execute `run diagnostics extended slot <slot>` command right after switch initialization.

Table 20: Resolved Issues, Platform-Specific and Feature Issues in ExtremeXOS 15.3.3 (Continued)

ID Number	Description
PD4-4164720240	ISIS hello packets are dropped when its IP-MTU size is greater than 1,500.
PD4-3494126219	Need CLI option in VPLS to tunnel Layer 2 control packets (LACP, EDP, STP, etc.) across VPLS cloud.
PD4-4161804048	MLAG bulksync needs to be optimized to reduce sync frequency.
PD4-4076099271	ACL rule to match all IPv6 packets is incorrectly matching all other packets, as well when match condition “source-address ::/0” is used.
PD4-4156882976	Process HAL ends unexpectedly with signal 11 after deleting MLAG peer on a switch with a PVLAN configuration.
PD4-4192894778	PVLAN + MLAG: HAL process ends unexpectedly during VRRP failover, if VRRP is enabled on a network VLAN with an isolated subscriber and the ISC link port is part of that network VLAN.
PD4-4072824510	With VLAN aggregation configuration, switch proxies GARP packet to the same sub-VLAN on which it is received, which in turn creates an IP conflict.
PD4-4086322381	IPv6 routes learned by BGP are not reachable even though they appear in the output of the `show iproute ipv6` command.
PD4-4112813573	Incomplete kernel log messages appear in the output of the `show log` command.
PD4-4046767881	A new command is required to refine the default link scan interval.
PD4-3912092557	When configuring EAPS ring ports, which are also remote mirror ports, errors occur.
PD4-3996186238	Attaching access-lists having UDF-based rules to multiple ports occupies a large amount of kernel memory.
PD4-3967545390	Process "dcbgp" ends unexpectedly when creating a BGPv6 neighbor with IPv6 addresses of lengths greater than 32 characters.
PD4-3872943883	Traffic originating from an ESRP master switch to the host attached to an ESRP slave switch fails when host attach port is part of two different ESRP domains that reside in the same ESRP group.
PD4-3844923871	The kerberos-related rules are not uninstalled after kerberos detection is triggered.
PD4-3767600099	Some VPNv4 routes do not appear after enabling or disabling the port.
PD4-4013926861	LACP PDUs not tunneled using L2PT feature.
PD4-3951874885	The configuration created by the command `enable netlogin dot1x guest-vlan ports <port no>` disappears after rebooting the switch.
PD4-3955776746	Loops are created after disabling or enabling VLANs that contain ports with the software redundant port feature enabled.
PD4-3953549295	Process climaster ends unexpectedly when commands like `configure`, `clear`, and `show`, which have an enter option after them are executed in legacy CLI mode.

Table 20: Resolved Issues, Platform-Specific and Feature Issues in ExtremeXOS 15.3.3 (Continued)

ID Number	Description
PD4-3955966044	Error messages occur while receiving LACP marker PDUs from other vendors' products.
PD4-3955966205	The process rtmgr ends unexpectedly with signal 11 when disabling/enabling ports in switches with VRRP configuration.
PD4-3938573731	Protocols deleted from user-created VRs stay at "STOPPED" state. An error message appears while trying to save the configuration.
SummitStack	
PD4-4192894838	In Summit stacks, temporary loops occur for a short time in EAPS rings either when a process ends unexpectedly in backup/ standby node or during a slot failover.
PD4-3996625741	In Summit stacks, some slots stay in "FDB sync" state after the stack is rebooted.
Summit X440 Series Switches	
PD4-4010837576	Spurious fan failure messages are logged even though fan is in working condition.
Summit X460 Series Switches	
PD4-4203383621	Summit X460 series switches with XGM3 modules stop responding occassionally when accessing registers or during execution of commands from the debug shell.
PD4-3955966396	Screenplay does not display device images.
PD4-3999505189	In Summit X460 series switches, the 10G links from XGM modules flap at random times.
Summit X650 Series Switches	
PD4-4155292955	In Summit X650-24x switches, VIM1-10G8X-1 stops sending the traffic after the error logs "<Erro:Kern.Error> smbus_wait_rdy: timeout waiting for SMBUS" "<Erro:HAL.Sys.Error> Error reading from XEN card eeprom (1, 83)".
PD4-4045085848	Packets are dropped due to congestion when sending more than 16GB traffic via VIM3-40G4X modules.
BlackDiamond 8800 Series Switches	
PD4-4215831631	HAL process signal 10 ends unexpectedly during a MSM failover with ACL redirect-port policy file.
PD4-4215712361	The process rtmgr signal 11 ends uenxpectedly when executing the commands `show iproute mpls` and `disable/enable mpls`.
PD4-3827836443	ACL process ends unexpectedly while applying 512 egress ACL rules to a port on the 8900-10G24X-c module.
PD4-4028210379	Ports stop forwarding traffic when egress mirroring is configured in some other port.
PD4-4007140987	ABR stops translating AS external routes (type 7) to another area (type 5) after OSPF is configured with graceful restart.

Table 20: Resolved Issues, Platform-Specific and Feature Issues in ExtremeXOS 15.3.3 (Continued)

ID Number	Description
BlackDiamond X8 Series Switches	
PD4-4214760373	Fabric modules go into failed state during bootup with error message " CardExec (state DIAG) timed out".
PD4-4215831516	During reboot, fabric modules are timing out in RT_SYNCED state and go to failed state.
PD4-4215830962	Backup management modules report all I/O modules are stuck in the "RT sync" state, even though they are actually operational.
PD4-3984146477	The error message "bcm_vlan_port_get failed" appears in the output of CLI command `debug hal show switch-manager vlan`.
PD4-3976741949	FPGA version and bootROM version do not appear correctly even after upgrading.

Resolved Issues in ExtremeXOS 15.3.2-Patch1-2

The following issues were resolved in ExtremeXOS 15.3.2-Patch1-2. ExtremeXOS 15.3.2-Patch1-2 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, ExtremeXOS 11.5.2.10, ExtremeXOS 11.6.5.3, ExtremeXOS 12.0.5, ExtremeXOS 12.1.7, ExtremeXOS 12.2.2-patch1-12, ExtremeXOS 12.3.6, ExtremeXOS 12.4.5, ExtremeXOS 12.5.5, ExtremeXOS 12.6.3, ExtremeXOS 12.7.1, ExtremeXOS 15.1.3, ExtremeXOS 15.2.2 and ExtremeXOS 15.3.1. For information about those fixes, see the release notes for the specific release.

Table 21: Resolved Issues, Platform-Specific and Feature Issues in ExtremeXOS 15.3.2-Patch1-2

ID Number	Description
General	
PD4-3890560446	Ingressed packets are dropped in Summit X670v and BlackDiamond X8 series switches.
PD4-3936248156	Restart timer configuration appears in the command `show config esrp` output even if it is as same as the default value.
PD4-3557170689	OSPFv3 neighborship is not established across an MPLS L2VPN cloud when a service VLAN port is part of another VLAN where the IPv6 address is configured.
PD4-3797678328	Renaming VLANs with same name as an existing user-created virtual-router should not be allowed.
PD4-3770392563	Kernel error message appears while configuring CEP translation for two different VMANs with same port and same target VLAN IDs.
PD4-3759280373	Disabling and enabling sharing of a LAG port in a VRRP-enabled VLAN should be allowed without requiring the disabling of VRRP.

Table 21: Resolved Issues, Platform-Specific and Feature Issues in ExtremeXOS 15.3.2-Patch1-2 (Continued)

ID Number	Description
PD4-3908211876	Six ARP requests are generated for every packet with an unknown destination. This should be reduced to two ARP requests, since in a VLAN-aggregation environment this can generate lot of requests
PD4-3910923973	In MLAG with LACP setup, rebooting one of the peers causes flapping of the LACP-sharing link connected to the MLAG port of the other peer.
PD4-3831014382	Secondary IP addresses for VLANs are unusable after deletion and re-configuration of any other existing secondary IP addresses in the same VLAN.
PD4-3854381445	The snmpMaster process ends unexpectedly when accessing a switch via a user created from the network monitoring tool.
PD4-3877669831	IP addresses are truncated in a switch's log message when SNMP walk is done with a bad community name.
PD4-3723545733	OSPFv3 stub nosummary is not working/configurable.
PD4-3845572495	Packet drop occurs in MLAG when removing a port from the aggregator.
PD4-3829770571	Egress mirroring does not work for CPU-generated packets when the mirrored and mirroring ports reside on different units.
PD4-3887166906	OSPF sends LS update packets with checksum 0xffff.
PD4-3790207675	Changing OSPFv3 timers to area 0.0.0.0 affects all areas.
PD4-3865215149	System ACL rules corresponding to IP multicast control packets is not uninstalled even after executing the command `configure ipmcforwarding to-cpu off port <all ports>`.
PD4-3896401521	Need a command to configure a source IP to send an XML notification.
Summit Family Switches	
PD4-3816761481	OSPF neighborship over L2VPN fails when an IGMP snooping filter per VLAN is configured on the switch.
PD4-3851670525	Summit switches does not display power usage with the `show power detail` command when a redundant power supply is unplugged, and then plugged back in.
Summit Stack	
PD4-3784189712	Part Information for stack node power supplies does not appear, or is only partially visible, in the `show power detail` command from the master.
PD4-3897318632	In the backup node of a Summit stack, the port corresponding to VSM process is always in the listening state, irrespective of MLAG configuration.
Summit X460 Series Switches	
PD4-3844769679	The traffic for other existing VPLS instances is affected on LAG ports when deleting a VPLS instance.

Table 21: Resolved Issues, Platform-Specific and Feature Issues in ExtremeXOS 15.3.2-Patch1-2 (Continued)

ID Number	Description
BlackDiamond 8800 Series Switches	
PD4-3925373055	ACL rules are not installed with ip-security enabled. This problem does not occur if ip-security is enabled after installing ACLs.
PD4-3927559233	Port Isolation does not seem to work on BlackDiamond 8800 series switches.
PD4-3836341924	When distributed ARP mode is enabled with many ARP entries, the next hop MAC addresses in the hardware are programmed incorrectly causing L3 reachability issues.
BlackDiamond X8 Series Switches	
PD4-3812895988	LACP ports do not become active after enabling the ports.
PD4-3887135847	Fan module part numbers and revision numbers appear as “N/A” or corrupt with random values after rebooting.

Resolved Issues in ExtremeXOS 15.3.2

The following issues were resolved in ExtremeXOS 15.3.2. ExtremeXOS 15.3.2 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, ExtremeXOS 11.5.2.10, ExtremeXOS 11.6.5.3, ExtremeXOS 12.0.5, ExtremeXOS 12.1.7, ExtremeXOS 12.2.2-patch1-12, ExtremeXOS 12.3.6, ExtremeXOS 12.4.5, ExtremeXOS 12.5.5, ExtremeXOS 12.6.3, ExtremeXOS 12.7.1, ExtremeXOS 15.1.3, ExtremeXOS 15.2.2 and ExtremeXOS 15.3.1. For information about those fixes, see the release notes for the specific release.

Table 22: Resolved Issues, Platform-Specific and Feature Issues in ExtremeXOS 15.3.2

ID Number	Description
General	
PD4-3790130061	FDB process ends unexpectedly with signal 11 when rebooting the MLAG peer.
PD4-3694263467	Fetching SNMP variable "extremeCpuMonitorSystemUtilization5mins" gives incorrect value.
PD4-3639991908	Connectivity on a VLAN port is lost when that port is deleted from a VMAN that it belongs to.
PD4-3494330102	Port congestion counter increments for a port that receives IGMP leave on a port.
PD4-3427549640	CPU utilization on BlackDiamond 8800 and Summit X670 series switches is high when you configure 256 PVST+ domains with 10 or more active links.

Table 22: Resolved Issues, Platform-Specific and Feature Issues in ExtremeXOS 15.3.2 (Continued)

ID Number	Description
PD4-3107133811	Kernel oops crash in expkt_packet_sock_destruct after performing command `restart process gptp`.
PD4-3075940603	DHCPv6 control packets are CPU-forwarded, rather than forwarded via the hardware.
PD4-3643342051	The CDP Hold-Timer is not resetting after disabling or enabling ports.
PD4-3638252379	Configuring ESRP HA port to multiple VLANs in the same group should not be allowed.
PD4-3448427351	The commands are not getting completed for "cfgmgr" modules after you press the **TAB** key.
PD4-3539122967	LocalAAA-Create account accepts the illegal character password `<a&>` for config account user <account name>. This should return an invalid token.
PD4-3747603651	ELRP disabled ports appear as "enabled" on ScreenPlay.
PD4-3452986361	BFD protocol should support IPv6 for single-hop sessions.
PD4-3421465775	Process dot1ag ends unexpectedly with signal-11 when disabling ERPS ring after enabling CFM debug-data level log.
PD4-3668906188	Hardware CFM is not detecting remote MEP-down event.
PD4-3447946575	CLI stops responding or ACL process ends unexpectedly when refreshing ACL policies containing rules that can fill up ACL hardware resources.
PD4-3705853485	The command `jerry show cli commands` displays an infinite list of repeated commands.
PD4-3582474967	CliMaster process ends unexpectedly while enabling OpenFlow in the SSH-enabled switches.
PD4-3514769636	The commands `enable pim snooping`, `disable pim snooping`, `enable cli space-completion` and `disable cli space-completion` produce ambiguity errors.
PD4-3427500331	The files under cyrus-sasl/mac are only needed when building for Apple/Mac platforms.
PD4-3466891441, PD4-3551981591	TACACS+ and RADIUS shared secrets do not allow '&' or '<' characters in configuration. **NOTE:** This issue is also fixed for all account passwords.
Summit Family Switches	
PD4-3519601013	Multicast packets are getting software-forwarded for groups that receive IGMP join or leave message, although there are other active receivers. This happens when there is no Source(S,G) tree and the traffic is switched via only RP(*, G) tree. The reprogramming can result in additional latency (with low data rates) and packet drops with high data rates.
PD4-3648806461	UNH TEST: gPTP.com.c.15: Common: MDPdelayReq State Machin
PD4-3585714011	Check for gPTP destination MAC address on packet receive, along with ethertype check, instead of just ethertype check.
PD4-3648806476	Ports are incorrectly removed from multi-port MAC entries.

Table 22: Resolved Issues, Platform-Specific and Feature Issues in ExtremeXOS 15.3.2 (Continued)

ID Number	Description
PD4-3747290387	In Summit stacks, false fan failure SNMP traps are triggered.
PD4-3769693861	Stack failover time takes around two seconds.
PD4-3562361721	In Summit X460 stacks, backup does not get config sync'd, when forming a stack with only one stacking port using alternate stacking mode.
PD4-3393943082	Issue 1: Observed the following error message after saving, and then rebooting Summit X460/480 series switches with auto on speed 1000/100 duplex half: <Erro:cm.sys.actionErr> Error while loading "ports": Half duplex is not supported on port 1. Issue 2: BASET link is coming up with auto on speed 1000 after saving and then rebooting Summit X460/480 series switches with auto on speed 100 duplex half.
PD4-3392413920	On V80 stack Summit X460-48x series switches with XGM3-2sf and x440-24t/48p modules, when BASET SFP (SFP+ passive copper cable) is inserted and then removed on that same port, the link is not becoming active.
PD4-3626405155	When MVRP initially adds a port to a VLAN, it simulates receiving a New, which results in propagating a New event, and eventually sending a New event. While this works, per the standard, if you receive a Join, you should propagate a Join. There are several MRP failures for which this is probably the cause.
PD4-3624043226	Handling for MVRP future protocol versions is not implemented.
PD4-3624043235	Do not forward frames with MVRP MAC DA.
PD4-3632022937	Need to handle both invalid 3-packed events and invalid leave-all events for both MVRP and MSRP.
PD4-3624043256	Listener de-registration proxy not currently implemented.
PD4-3632022997	Need to delete the reservation in the Leave action, and not wait until the attribute is deleted. If TA goes MT, need to fail Listener and delete reservation.
PD4-3582467381	System ends unexpectedly when running 298 listeners and 294 talkers.
PD4-3634065171	Transmitted LeaveAll causes registrations to expire (domain).
PD4-3605702391	Should not propagate a Talker Advertise while the DUT.TS1 port is untagged.
PD4-3553141073	Ignore the reserved field in the talker message and reset to zero.
PD4-3624043244	Should not forward MSRP MAC addresses (even if the etherType does not match the MSRP etherType).
PD4-3624043264	Need to implement handling for future MSRP versions.
Summit X440 Series Switches	
PD4-3470086981	On Summit X440 series switches, Tx/Rx flow control is not working.
PD4-3473404958	Mirroring fails after a save and reboot when an active port is configured as a loopback port.

Table 22: Resolved Issues, Platform-Specific and Feature Issues in ExtremeXOS 15.3.2 (Continued)

ID Number	Description
PD4-3750514597	Summit X440-48p series switches are not delivering power on enabling following modules: SSH2, QoS, Diffserv, and LLDP.
Summit X450 Series Switches	
PD4-3492094131	On Summit X450a series switches with XGM2-2xf modules, the `show ports <port list> transceiver information detail` command output is not working on DDMI supported optics (XFP, SFP+). This problem appears in the following builds: ExtremeXOS 15.3.1, 15.2.2.7, 15.2.2.6, 15.2.2.5, and 15.2.2.4 (*not* observed with 15.1.2.12).
Summit X460 Series Switches	
PD4-3556682410	Rx CRC is incrementing when traffic passes through 10 meter 10G DA passive copper cables.
Summit X670 Series Switches	
PD4-3723545680	Enabling or disabling AVB causes “Erro:HAL.PTP.Error”.
PD4-3734509671	Known unicast traffic is not shared between the stacking ports when v320 G stacking is enabled.
BlackDiamond BX8 Series Switches	
PD4-3555060811	SNMP get on bgp4PathAttrTable returns value for routes from only one peer even though there are routes from multiple peers.
PD4-3555060904	SNMP get for BgpPeerTable produces error: `Lexicographical ordering error detected`
PD4-3741258577	BFD stuck in pending state for OSPFv3 neighbors.
PD4-3766693351	OSPFv3 ends unexpectedly with signal 11.
PD4-3710524777	Static-mac-move notification can create the following message notification in log: “<6>everestBcmpktToSkb: Could not get pif for slot=2 port=-1”
PD4-3397742865	Link fails to come up after changing a port from a 1000BaseT SFP optic to a 10GBaseX SFP+ optic.
BlackDiamond 8800 Series Switches	
PD4-3742983190	Process mcmgr ends unexpectedly in MLAG peer switch when an ISC is added as a router port.
PD4-3604039914	Process devmgr ends unexpectedly with signal 5 after switch restarts.
PD4-3431916827	System ends unexpectedly with "Process hal pid 1274 died with signal 11" error message when executing the command `debug hal show dwdmChannel slot 2 port 45` on BlackDiamond 8800 series switches with 8900-10G4X-xl io cards.

Table 22: Resolved Issues, Platform-Specific and Feature Issues in ExtremeXOS 15.3.2 (Continued)

ID Number	Description
E4G Cell Site Routers	
PD4-3501679501	Bit errors occur on TDM ports that use clocks recovered adaptively from a CES pseudowire to time the data in the transmit direction.
PD4-2907412645	For E4G-200 cell site routers, in a multi-path topology, all routes (primary and alternate) get withdrawn from the VPNv4 route table when one of the paths goes down.
BGP	
PD4-3725114681	As-path for the dampened routes does not appear in output from `show bgp neighbor` command.
PD4-3568617991	In BGP, executing the command `enable bgp peer-group p1 capability ipv4-unicast` produces the following error: `Error: missing close-brace and the cli does not work`
PD4-3615139364	The process dcbgp ends unexpectedly while deleting disabled ibgp peer after BGP process restart.
IP Routing Protocols	
PD4-3298891721	PIMv6: Traffic drop occurs when all ports are restarted on a LHR/RP connected to a multi-access VLAN.
PD4-3289104822	PIMv6: Intermittently, routers running in dense mode stop forwarding all received traffic when ports are restarted on the PMBR neighbor.
PD4-3444243381	PIM DR_Priority/PIM IPv6: No (S;G) appears on the RP, where a Summit X670 is the FHR and a BlackDiamond 8800 is the RP.
PD4-2825472985	L3VPN: failovers between LSPs take a long time—between 30–400 seconds.
PD4-3623434660	The VM image ends unexpectedly during load time.
SNMP	
PD4-2288889611	Snmpwalk results in lexicographic errors on Summit stack switches.
PD4-3508201981	The command `configure snmpv3 add target-addr C param hex A ipaddress 10.1.1.1/A transport-port 1 tag-list 1` produces ambiguity errors.
VLAN	
PD4-3747603776	Unable to delete the port from the VLAN via snmpset operation.

Resolved Issues in ExtremeXOS 15.3.1-Patch1-14

The following issues were resolved in ExtremeXOS 15.3.1-patch1-14. ExtremeXOS 15.3.1-patch1-14 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, ExtremeXOS 11.5.2.10, ExtremeXOS 11.6.5.3, ExtremeXOS 12.0.5, ExtremeXOS 12.1.7, ExtremeXOS 12.2.2-patch1-12, ExtremeXOS 12.3.6, ExtremeXOS 12.4.5, ExtremeXOS 12.5.5, ExtremeXOS 12.6.3, ExtremeXOS 12.7.1, ExtremeXOS 15.1.3, ExtremeXOS 15.2.2 and ExtremeXOS 15.3.1. For information about those fixes, see the release notes for the specific release.

Table 23: Resolved Issues, Platform-Specific and Feature Issues in ExtremeXOS 15.3.1-patch1-14

ID Number	Description
General	
PD4-3715756888	MLAG peers are checkpointing each other every minute when VRRP is enabled.
PD4-3707637261	OSPFv3 process ends unexpectedly at random times when switches have duplicate router ID in OSPFv3 network.
PD4-3701534347	When rules are falling under different slices, packets can match multiple rules and non-conflicting actions from the different slices are executed. For IPv6 traffic, if the packet matches a permit condition as well as a deny rule with mirror-to-cpu action, the IPv6 traffic packets get duplicated.
PD4-3665828866	In STP domains, temporary flooding should not get triggered during link-down events of ports configured with edge-safeguard.
PD4-3710524677	During authentication, a user rejected by a Radius/TACACS server should not get authenticated via local database.
PD4-3628368081	Applying access-profile to SSH2 produces an error.
PD4-3689508953	When the rules are falling under different slices, packets can match multiple rules and non-conflicting actions from the different slices are executed. In the case of ARP, if the packet matches a permit condition as well as a deny rule with mirror-to-CPU action, the ARP packets get duplicated.
PD4-3604171118	Switch console/Telnet session stops responding when executing any command after clicking the **save config** tab in ScreenPlay.
PD4-3657864343	In CLI scripting, $READ statements in both IF and ELSE conditions are executed at the same time even though only one of IF/ELSE condition is satisfied.
PD4-3687171749	In `show log` output the peer-id logged for MLAG port events is different from the configured peer-id.
PD4-3582809070	The command `disable ip-security arp learning learn-from-arp vlan <vlan_name> ports <ports>` appears incorrectly in `show configuration`.
PD4-3743455935	STP port status moves from "Blocking" to "Forwarding" state when a VLAN tag is changed.

Table 23: Resolved Issues, Platform-Specific and Feature Issues in ExtremeXOS 15.3.1-patch1-14 (Continued)

ID Number	Description
PD4-3732047131	ARP request packets for a specific pair of IP addresses does not egress out of LAG ports.
PD4-3765695234	Kernel oops occurs when continuous IP ARP addition/deletion happens during execution of `show tech` command.
PD4-3735477863	Jumbo frame-sized packets were not fragmented and hence dropped if ingress port and egress LAG member port are on the same unit.
E4G Cell Site Routers	
PD4-3211428714	In normal Layer-2 VLAN TDM, UDP PW traffic is forwarded to the CPU, unless ipforwarding is enabled or loopback is enabled on the VLAN. Need a CLI check to ensure customer enables ipforwarding on VLANs that have TDM IP PW.
PD4-3714872874	E4G cell site routers fail while executing a command without TDM module.
PD4-3178218438	For E4G cell site routers, TDM/UDP-PW/UDP port warning messages are not gettting logged for port 1024 and higher.
Summit Family Switches	
PD4-3598279043	In Summit stacks, after failover the backup node stays in down state and other nodes go to failed state.

Resolved Issues in ExtremeXOS 15.3.1-Patch1-10

The following issues were resolved in ExtremeXOS 15.3.1-patch1-10. ExtremeXOS 15.3.1-patch1-10 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, ExtremeXOS 11.5.2.10, ExtremeXOS 11.6.5.3, ExtremeXOS 12.0.5, ExtremeXOS 12.1.7, ExtremeXOS 12.2.2-patch1-12, ExtremeXOS 12.3.6, ExtremeXOS 12.4.5, ExtremeXOS 12.5.5, ExtremeXOS 12.6.3, ExtremeXOS 12.7.1, ExtremeXOS 15.1.3, ExtremeXOS 15.2.2 and ExtremeXOS 15.3.1. For information about those fixes, see the release notes for the specific release.

Table 24: Resolved Issues, Platform-Specific and Feature Issues in ExtremeXOS 15.3.1-patch1-10

ID Number	Description
General	
PD4-3665028748	STP: Spanning-tree participation is lost for a trunk after switch reboot.
BlackDiamond X8 Series Switches	
PD4-3558231182	On BlackDiamond X8 series switches, ACL policies with match conditions like "arp-sender-address" or "arp-target-address" do not work.

Resolved Issues in ExtremeXOS 15.3.1-Patch1-9

The following issues were resolved in ExtremeXOS 15.3.1-patch1-9. ExtremeXOS 15.3.1-patch1-9 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, ExtremeXOS 11.5.2.10, ExtremeXOS 11.6.5.3, ExtremeXOS 12.0.5, ExtremeXOS 12.1.7, ExtremeXOS 12.2.2-patch1-12, ExtremeXOS 12.3.6, ExtremeXOS 12.4.5, ExtremeXOS 12.5.5, ExtremeXOS 12.6.3, ExtremeXOS 12.7.1, ExtremeXOS 15.1.3, ExtremeXOS 15.2.2 and ExtremeXOS 15.3.1. For information about those fixes, see the release notes for the specific release.

Table 25: Resolved Issues, Platform-Specific and Feature Issues in ExtremeXOS 15.3.1-patch1-9

ID Number	Description
General	
PD4-3624802516	VMT process ends unexpectedly with signal 11 and the device reboots when enabling VM-tracking on Ridgeline.
PD4-3604668901	Changing ACL rule-compression port counters mode from "shared" to "dedicated" does not take effect even after unconfiguring/reconfiguring all ACL policies.
PD4-3603702268	In EAPS, when segment ports and shared ports are disabled and then enabled in quick succession, sometimes the segment port can remain blocked for up to 10 seconds.
PD4-3624118183	Missing a semicolon after mirror-cpu action modifier causes the ACL process to end unexpectedly even though check policyreports is successful.
PD4-3621148511	VMAN traffic egressing LAG ports is suppressed if LAG ports are configured to use secondary ethertype.
PD4-3583969250	Configuring SNMP community name with special characters is getting rejected.
PD4-3600411962	When a load sharing port is added to five or more STP domains, the command `show sharing details` output has the error "Error: Missing inputs, cannot process," and it is not showing more than five STP domains.
PD4-3649152517	Sharing not formed with VIM ports when the switch comes up for the first time with the VIM. Also the error message does not convey what the problem is.
PD4-3649152388	VSM memory leak occurs on backup slot during link state changes.
PD4-3631674565	HAL memory leak occurs while flapping VRRP backup.
PD4-3650508477	Switch incurs parity errors and traffic loss from LAG.

Table 25: Resolved Issues, Platform-Specific and Feature Issues in ExtremeXOS 15.3.1-patch1-9 (Continued)

ID Number	Description
Summit X440 Series Switches	
PD4-3657842888	On Summit X440 series switches, slot reboots after sending multicast packet from one node to another when the egress port speed is slower than the ingress traffic rate.
Summit X650 Series Switches	
PD4-3616193001	On Summit X650 series switches with vim3-40Gx modules installed, an error occurs when enabling rate limit on any port.
BlackDiamond X8 Series Switches	
PD4-3607636716	While using DAD to detect duplicate IP addresses, DAD does not get completed and duplicate IP addresses are not detected.
BlackDiamond 8800 Series Switches	
PD4-3639450097	Some MAC addresses are not checkpointed between MLAG peers after a switch reboot.

Resolved Issues in ExtremeXOS 15.3.1-Patch1-7

The following issues were resolved in ExtremeXOS 15.3.1-patch1-7. ExtremeXOS 15.3.1-patch1-7 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, ExtremeXOS 11.5.2.10, ExtremeXOS 11.6.5.3, ExtremeXOS 12.0.5, ExtremeXOS 12.1.6, ExtremeXOS 12.2.2-patch1-12, ExtremeXOS 12.3.6, ExtremeXOS 12.4.5, ExtremeXOS 12.5.4, ExtremeXOS 12.6.2, ExtremeXOS 12.7.1, ExtremeXOS 15.1.2, ExtremeXOS 15.2.1, and ExtremeXOS 15.2.2. For information about those fixes, see the release notes for the specific release.

Table 26: Resolved Issues, Platform-Specific and Feature Issues in ExtremeXOS 15.3.1-patch1-7

ID Number	Description
General	
PD4-3564943875	Summit stacks in ring mode get converted to daisy-chain mode or dual master state after rebooting. This happens when stacking is formed using alternate stack ports with SFP+ optics from SumitomoElectric and OpNext vendors.
PD4-3370824571	Configuration for netlogin authentication failure VLAN is lost after rebooting.
PD4-3579843238	Manual ESRP failover exceeds neighbor time-out instead of normal hello time-out.
PD4-3577171510	CliMaster process ends unexpectedly after logging on and off the switch multiple times.

Table 26: Resolved Issues, Platform-Specific and Feature Issues in ExtremeXOS 15.3.1-patch1-7 (Continued)

ID Number	Description
PD3-93829391	Configurations using a VR-Mgmt interface as a RADIUS client IP may not load at boot-up. However, using an interface in VR-Default does load correctly.
PD4-3451924367	CLI Scripting produces incorrect error message while trying to access non-existing argument.
PD4-3431916948	ESRP dual SLAVE state occurs, when a physical loop is detected in switch having "elrp-premaster-poll" and "elrp-master-poll" configuration.
PD4-3489840135	In `show configuration esrp` output, "count" and "interval" arguments of elrp-premaster-poll configuration appear in swapped order.
PD4-3489840224	An incorrect error message appears while unconfiguring dhcp-options.
PD4-3448586421	The log message "unspecified Nexthop. Not downloading Route" appears continuously since OSPFv3 does not retry downloading a route with an unspecified gateway next hop.
PD4-3518192174	The telnetd process is not re-started on executing `restart process telnetd` from a telnet session.
PD4-3444143389	CPU utilization value is not normalized on platforms with multi-core CPUs.
PD4-3417486171	Logon to the switch via XML and Web-based Netlogin is not working.
PD4-3473499277	IP address of the system does not appear in the switch log message while logged on through ScreenPlay (XML).
PD4-3506684608	Dynamic ACL entry for a port is not flushed until the DHCP snoop entry is cleared with source-ip-lockdown enabled.
PD4-3447946710	The process rtmgr ends unexpectedly while updating routing table with IBGP, OSPF routes learned from two different gateways.
PD4-3554903905	PoE process ends unexpectedly when executing `show inline-power info detail ports <port list>` command.
PD4-3517009825	Routes are not advertised to EBGP peer after restarting BGP process.
PD4-3518631249	Packet statistics are not displayed on aborting Ping/Traceroute.
PD4-3492560474	ISIS LSP not advertised to the peer when switch receives same LSP within a short interval.
PD4-3494590960	SNMP Trap is not sent when a fan module is removed from switch.
PD4-3496956716	The command `show configuration` output is not showing QP1 QoS Profile.
PD4-3496956761	Nettools process ends unexpectedly while forwarding DHCPv6 packets over the 6-in-4 tunnel.
PD4-3435560331	ACL process crash ends unexpectedly while deleting/creating meters and simultaneously executing `show meter` command from other telnet session.

Table 26: Resolved Issues, Platform-Specific and Feature Issues in ExtremeXOS 15.3.1-patch1-7 (Continued)

ID Number	Description
PD4-3531064078	When enabling LAG and VLAN translations together, L2 broadcast traffic is not forwarded to the LAG ports by the switch.
PD4-3449497221	Need CLI command to ignore PIM neighborship check for the ingress multicast traffic in PIM dense mode.
PD4-3554134901	The process snmpSubagent ends unexpectedly with signal 6 while retrieving one of the variable in the ifentry.
Summit Series Switches	
PD4-3469160626	On Summit X440 and X460 switches, links remain down on ports with these settings: “speed 1000/half-duplex/auto-negotiation on”.
Summit NWI-E450A Switches	
PD4-3457486046	NWI-E 450A: No log message occurs when switch temperature exceed maximum value.
Summit X440 Series Switches	
PD4-3483801581	On Summit X440 stack switches, “i2c-1: shid_eeprom_tlv_readv” warning messages appear during bootup.
PD4-3433391566	On Summit X440 stacks, the temperature form stack node is not displayed properly.
Summit X460 Series Switches	
PD4-3578903800	ERPS with ELSM malfunctioning when CFM/CCM is enabled.
PD4-3423025150	Unicast packet are getting dropped while passing through Summit X460 stacking.
PD4-3484451058	MAC address is not learned by the switch while sending LLC packets.
Summit X650 Series Switches	
PD4-3494126184	On Summit X650 switches, VRRP hello with advertisement 0 is sent while disabling and enabling the links on VRRP master.
Summit X670 Series Switches	
PD4-3434390931	On Summit X670V-48x switches with VIM4-40G4X module, kernel error messages "Disabling IRQ" appear during bootup.
BlackDiamond 8800 Series Switches	
PD4-3519894139	With VPLS configuration, FDB entries are missing from hardware after slot reboot.
PD4-3517121527	Remote mirroring on a source switch is enabling software learning after rebooting the switch with the configuration.

Table 26: Resolved Issues, Platform-Specific and Feature Issues in ExtremeXOS 15.3.1-patch1-7 (Continued)

ID Number	Description
BlackDiamond X8 Series Switches	
PD4-3579052669	Power budget calculation is not accurate in the in the output of the `show power budget` command.
PD4-3585522991	SCREENPLAY: Temperature row displays "RED" even when the slots are running under recommended normal temperature level (25 to 100 C).
PD4-3489997111	On BlackDiamond X8 series switches, execution of the CLI command `show log message nvram` is very slow.
E4G Cell Site Routers	
PD4-3468165415	Traffic on SAToP CES pseudowire goes down when adding an ACL to an uplink port.

Resolved Issues in ExtremeXOS 15.3.1-Patch1-3

The following issues were resolved in ExtremeXOS 15.3.1-patch1-3. ExtremeXOS 15.3.1-patch1-3 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, ExtremeXOS 11.5.2.10, ExtremeXOS 11.6.5.3, ExtremeXOS 12.0.5, ExtremeXOS 12.1.6, ExtremeXOS 12.2.2-patch1-12, ExtremeXOS 12.3.6, ExtremeXOS 12.4.5, ExtremeXOS 12.5.4, ExtremeXOS 12.6.2, ExtremeXOS 12.7.1, ExtremeXOS 15.1.2, ExtremeXOS 15.2.1, and ExtremeXOS 15.2.2. For information about those fixes, see the release notes for the specific release.

Table 27: Resolved Issues, Platform-Specific and Feature Issues in ExtremeXOS 15.3.1-patch1-3

ID Number	Description
General	
PD4-3447784385	Log messages are not generated for some MLAG events though they are configured in log filter.
BlackDiamond 8800 Series Switches	
PD4-3555470737	On BlackDiamond 8800 series switches, traffic fails to switch over to next available gateway after removing Master MSM physically.

Resolved Issues in ExtremeXOS 15.3.1-Patch1-2

The following issues were resolved in ExtremeXOS 15.3.1-patch1-2. ExtremeXOS 15.3.1-patch1-2 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, ExtremeXOS 11.5.2.10, ExtremeXOS 11.6.5.3, ExtremeXOS 12.0.5, ExtremeXOS 12.1.6, ExtremeXOS 12.2.2-patch1-12, ExtremeXOS 12.3.6, ExtremeXOS 12.4.5, ExtremeXOS 12.5.4, ExtremeXOS 12.6.2, ExtremeXOS 12.7.1, ExtremeXOS 15.1.2, ExtremeXOS 15.2.1, and ExtremeXOS 15.2.2. For information about those fixes, see the release notes for the specific release.

Table 28: Resolved Issues, Platform-Specific and Feature Issues in ExtremeXOS 15.3.1-patch1-2

ID Number	Description
General	
PD4-3485029693	The following error appears in the debug shell: "soc_l2x_thread: DMA failed: Operation failed". Occurs on Summit X450, X460, X650, X670, and BlackDiamond X8 series switches.
Summit X460 Series Switches	
PD4-3550015329	On Summit X460 series switches, HSRP MAC address is not learned on both switching units.
PD4-3553665326	On Summit X460 series switches, certain MAC addresses like HSRP/VRRP are not re-learned after STP-triggered FDB flush events.

Resolved Issues in ExtremeXOS 15.3

The following issues were resolved in ExtremeXOS 15.3. ExtremeXOS 15.3 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, ExtremeXOS 11.5.2.10, ExtremeXOS 11.6.5.3, ExtremeXOS 12.0.5, ExtremeXOS 12.1.6, ExtremeXOS 12.2.2-patch1-12, ExtremeXOS 12.3.6, ExtremeXOS 12.4.5, ExtremeXOS 12.5.4, ExtremeXOS 12.6.2, ExtremeXOS 12.7.1, ExtremeXOS 15.1.2, ExtremeXOS 15.2.1, and ExtremeXOS 15.2.2. For information about those fixes, see the release notes for the specific release.

Table 29: Resolved Issues, Platform-Specific and Feature Issues in ExtremeXOS 15.3

ID Number	Description
General	
PD4-3271412898	Some IPv4/IPv6 multicast streams received on a Summit X670 stack are not sent out on egress ports. The egress port is 40G LAG and ingress port is a 10G LAG. mcast cache, HAL and hardware are programmed correctly, but traffic does not egress on 40G LAG ports.
PD4-3253491193	DHCPV6Relay: Config upload/download .xsf on executing `unconfig switch all` and loading dhcpv6config makes interface ID show an invalid tag value than the configured tag value for the VLAN.
PD4-3415999201	EMS messages/events supported.
PD4-3420578731	Static CFM group association with ERPS ring fails after the ring is disabled/enabled.
PD4-2797829304	The command `show conf` does not show when SSH2 has been enabled.
PD4-3007653061	Quitting the command `show config` causes memory leaks.
PD4-3405669115	In some circumstances, filtering on a port for "FDB.MACTracking" is not logging any informational messages.
PD4-3357584975	System MAC for VLAN gets overwritten with dynamic MAC in case of hash collision, causing L3 reachability issues.
PD4-3404733334	Switch logs "Info:RtMgr.Server.ProcGetRtMsgFail" message appears frequently (every 30 seconds) when it tries to export an unfeasible route. Informational messages should appear less frequently.
PD4-3138803991	Switches stop working after deleting virtual-router vir_1. This issue occurs in ExtremeXOS 15.2.1 and 15.2.2.
PD4-3400038115	Multicast cache entries associated with router port get deleted after timer expires, if MVR is enabled.
PD4-3300114424	Ingressing local multicast traffic to the super-VLAN via sub-VLAN ports is sent back to the same port.
PD4-3314306583	IGMP general query dropped due to multicast loop detection.

Table 29: Resolved Issues, Platform-Specific and Feature Issues in ExtremeXOS 15.3 (Continued)

ID Number	Description
PD4-3118104426	OSPF process ends unexpectedly when moving a VLAN from one area to another area.
PD4-3199780495	Virtual link is not working in OSPF.
PD4-2202806910	OSPFv3 NSSA area configurations are not shown in the CLI command `show config ospfv3` and `show ospfv3 area`; OSPFv3 area type always remains in the Normal area.
PD4-2797679070	BGP config for VRF is not cleaned up after a VRF is deleted.
PD4-3330304088	VRRP process signal 6 ends unexpectedly while adding VLAN and VRRP instances.
PD4-2853885980	Hot plugging management cable with iPv6 address results in "exvlan_ioctl_handler:3036:" error messages in the logs and remains in the "Tentative" state.
PD4-3122862720	ELRP process with signal 6 ends unexpectedly when STP tries to disable a trunk port.
PD4-3328741256	ExtremeXOS 12.6.2.10: Port stops learning on a VLAN after limit learning is enabled on the VLAN.
PD4-3317958618	Packet loss up to two seconds occurs when one of the MLAG peer switch is rebooted.
PD4-3122863433	"hallsCardAlive-183 Slot 0" message appears at console when a trunk port is disabled by STP.
PD4-3170880275	MPLS packets are being forwarded in software instead of hardware on Summit X670, BlackDiamond X8, and BlackDiamond 8900-40G6X-xm when IP DAD is enabled, causing LDP sessions to drop/timeout.
PD4-3122863468	ARP requests are getting dropped due to the ARP validation when it is received from a DHCP-client.
PD4-3030089102	If TCP tracking for LAG port fails, and then becomes active, the LAG health-check remains down.
PD4-3227396996	NTP and DAD cannot co-exist. If you enable NTP and DAD on the same VLANs, and then reboot the switch by saving the configuration, the NTP configuration for VLANs is removed when switch comes back up.
PD4-3138242320	BFD-protected static route does not failover when the BFD session goes down.
PD4-3124148155	Refresh policy triggers ACL process to end unexpectedly while backing up MSM, and it goes out of sync.
PD4-3138604241	[10063] 100BASE (with phy) FX SFP optics link is not coming up after issuing command `config ports 9-11 auto off speed 100 duplex full` after saving and then rebooting Summit X440/ BlackDiamond 8800 series switches and although partner link is up. This issue is seen between the Summit X440 and X460. This issue occurs in ExtremeXOS: v1522b0-br-SR1-4, 15.2.1.5, and 15.1.2.12.
PD4-3176665990	Combo port does not come up with auto-negotiation off after reboot when preferred medium is configured.

Table 29: Resolved Issues, Platform-Specific and Feature Issues in ExtremeXOS 15.3 (Continued)

ID Number	Description
PD4-3204711497	On Summit X670v-48x series switches, Part Number and Serial Number are incorrect for 4th channel when configured in 4x10G mode. This issue also occurs on Summit X650, X480, and X670v.
PD4-3273707491	Rx jabber counter increments with jumbo frames.
PD4-2930580825	vmtFileFetch: execv() failed /usr/bin/wget -v 0 -O /tmp/vmt/MANIFEST when `run vm-tracking rep sync-now` command is executed and sometimes sync fails.
PD4-3136817360	Duplicated multi-cast packets appear while receiving J/P packets from LHR when a switch is acting as a assert-winner and a non-RP.
PD4-3184827915	IPMC forwarding configuration is corrupted after enabling license.
PD4-3178317084	Multi-cast packets are getting duplicated when source IP address is 0.0.0.0.
PD4-2841783640	`show bgp route address-family vpnv4 detail all` is showing label as part of the vpnv4 prefix.
PD4-3109325898	LAG member ports do not appear in `show ports tag <tag number>` command output.
PD4-3161130688	Need a way to turn off temporary flooding in STP domains using the CLI.
PD4-3234332590	STP process ends unexpectedly when restricted role is enabled in dot1d mode.
PD4-3250650157	After a radius authentication failure, you are unable to access the switch using failsafe account.
PD4-3237306270	DHCP snooping does not work if VLAN translation and ip-security are configured together on a switch.
PD4-3237904817	Unable to upload the dhcp-binding manually to the server.
PD4-3237904954	Error message occurs when uploading dhcp-binding to the server after changing the file name.
PD4-3199137619	Switch does not get model information (EVENT.DEVICE_MODEL) when an LLDP-enabled device is unplugged from the switch.
PD4-3128801005	After saving switch configuration with downloaded certificate, switch displays `Error Validating Certificate` error on thttpd restart.
PD4-3316990487	XML is not working with IPv6, making is you cannot manage the switch from web using an IPv6 address.
PD4-3267725700	ACL process ends unexpectedly when unconfiguring an access-list profile which has 32 characters.
PD4-3234332760	ACL refresh fails with error message - "unavailability of hardware resource or system error".
PD4-3160447091	After downloading and installing SSH module, `Image Selected` information from `show switch` command, changes back to the booted partition.
PD4-2678796534	If you use an ACL to mirror traffic to a port and then disable mirroring on that port, traffic continues to flow to that port.

Table 29: Resolved Issues, Platform-Specific and Feature Issues in ExtremeXOS 15.3 (Continued)

ID Number	Description
PD4-1996237147	The priority flow control is not disabled when using the `disable` command with the `all` option.
PD4-3234332692	SNMP OID for ExtremeportQP TxBytes always return 0.
PD4-3054251501	Typo: In the error message when adding a duplicate log filter in EMS, "your are" needs to be changed to "you are".
PD4-3298782274	SNMP query of extremeBootTime.0 returns a value in the local configured time zone instead of UTC.
PD4-3314659004	ISIS process ends unexpectedly while configuring interlevel-filter with a lengthy policy file name.
PD4-3314659087	OSPF process ends unexpectedly if a lengthy password is used.
PD4-3267770777	The number of blank lines printed under the RIP module of the `show configuration` command output increases with an increase in the number of Layer 3 VLANs.
PD4-3316937162	FDB process crashes while clearing neighbor-discovery cache
PD4-3078305908	"Failed to find_rtMgrClient_hash(0xFFFF000D)" error messages are logged, if netTools fails to register as route manager client on rare occasions after system reboot.
PD4-3273898398	NetTools process ends unexpectedly while displaying auto-provision for a virtual-router with a lengthy name.
PD4-3242760247	Manually configured ACL system application priority reduced by one for every reboot and more application seen in ACL zone.
PD4-3331822984	ACL process ends unexpectedly when creating flow-redirect with a large string for redirect-name.
PD4-3316990444	IPFIX configuration does not take the VR configuration into effect.
BlackDiamond 8800 Series Switches	
PD4-3134475729	Error message appears on the switch while disabling/enabling the slot with mirroring configuration.
PD4-2968093427	With BGP max peering, the `disable bgp neighbor all` command causes the switch to fail.
PD4-2582883670	Process DCBGP ends unexpectedly with signal 11 when trying to delete 100 inactive neighbors.
PD4-2931845350	Issuing CLI to enable and apply export policy to VPN VRF on PE (to existing configuration) returns this error: "Error: vr red: Cannot change export policy for protocol bgp while export is enabled"
PD4-3297769048	Switch-fabric egress port is getting deleted when pseudowire adds and deletes arrive out of order.
PD4-3193434741	On BlackDiamond 8800 series switches, when the number of packets queued for transmit by the CPU exceeds 500, additional slow path forwarded packets are dropped.
PD4-2051483560	The `show iproute summary` command output occasionally shows the non-zero number of compressed routes even though the routes are no longer there.

Table 29: Resolved Issues, Platform-Specific and Feature Issues in ExtremeXOS 15.3 (Continued)

ID Number	Description
PD4-3190863671	I/O module 10G4Xc goes to failed state after reporting "conduit asynchronous transmit error encountered," and then reboots.
PD4-3298782375	On BlackDiamond 8806 and 8810 series switches running ExtremeXOS 12.5 and later, I/O modules inserted in a dual-use slot (MSM or I/O slot) do not become operational.
PD4-3230196968	Executing "snmpwalk" operation on "pethMainPseTable" causes snmpMaster to end unexpectedly occasionally with signal 6.
BlackDiamond 10800 Switches	
PD4-3255799520	When an EAPS ring has multiples of 284 as protected VLANs, then ports are not blocked and can cause a traffic loop after rebooting the switch.
BlackDiamond X8 Series Switches	
PD4-3328224544	Counters for some VMs are not installed and the following error appears in log: "12/10/2012 11:10:04.33 <Erro:HAL.IPv4ACL.Error> MM-B: Rcv checkpoint - dynRuleInst for vlan=0 port=70018 NULL (rule xnv_ing_dyn_rule_007bb5b8ae)".
PD4-3415694835	FAN speed reaches 5,000 RPM after hot-swapping FAN modules and does not return to normal range (3,000 RPM).
PD4-3404733158	IDMGR process ends unexpectedly while binding a user with a lengthy password.
PD4-3178905992	40G24X modules fail with conduit errors when system is stressed with ARP requests/replies.
PD4-3199780261	DCBGP process ends unexpectedly while configuring IPv6 address to the VLAN which was associated with BGP.
PD4-3297768981	<Erro:HAL.MPLS.Error> MM-A: pibMplsPwUpdate pibMplsPwNhlfellmWrite failed with error -1., appears after `restart ports all.`
PD4-3144429723	MLAG-MLDv2: Record type for MLDv2 reports is modified after management module failover.
PD4-3282651251	The command `show ntp association` statistics does not display any output.
PD4-3092483367	ExtremeXOS image download is causing DOS-protect information when downloading over the gig connection.
PD4-3173100402	Spurious characters appear on console when enabling SFLOW.
PD4-3300086043	xmlc process ends unexpectedly while creating xml-notification with lengthy parameters.

Table 29: Resolved Issues, Platform-Specific and Feature Issues in ExtremeXOS 15.3 (Continued)

ID Number	Description
SummitStack	
PD4-3418269038	Process rtmgr ends unexpectedly with signal 6 on backup while rebooting neighboring switches. "01/16/2013 17:55:46.18 <Warn:RtMgr.Server.NtfyIpmlQFull> Slot-2: Notify IPML queue full. clnt=131138, ntfy peer-id=14. 01/16/2013 17:55:53.48 <Erro:RtMgr.Client.ReplyTimeOut> Slot-1: Client with ID=0x00020F09 Timed out waiting for (LKUPRPF). Process rtmgr pid 1530 died with signal 6 Code: 489eac 00000000 nop 489eb0 8c430094 lw v1,148(v0) 489eb4 8c640038 lw a0,56(v1) 489eb8 <1080001a>beq a0,zero,0x489f24 489ebc 00000000 nop 489ec0 8c830060 lw v1,96(a0) 489ec4 12430003 beq".
PD4-3334236490	On Summit V80 stacks, the following error message appears when booting up the stack without any configuration: "<Erro:HAL.Port.Error> Slot-1: Unable to get media type from slot 4 port 4 error -1".
PD4-2908405391	On SummitStacks, the following warning message appears while rebooting the stack: "<Warn:Kern.Card.Warning> Slot-1: pci 0000:02:00.1: warning: supported max payload size less than 256 bytes <Warn:Kern.Card.Warning> Slot-1: pci 0000:02:00.0: warning: supported max payload size less than 256 bytes". This issue does not occur in ExtremeXOS v15_2_0_21.
Summit Series Switches	
PD4-3432492701	Summit NWI-E450A platform cannot install the "320051jaguarsummitX-15.2.0.9-br-SDK601-11.xos" image.
PD4-3327782716	Summit X250e-24xDC series switches do not boot up with ExtremeXOS 15.2.2.7.
PD4-2879629222	Under certain conditions, large number of packet drops occur when traffic is failed over to other active member ports in the LAG.
PD4-3206781851	Fan tray failure error messages occur on Summit family switches.
PD4-3327782647	ExtremeXOS should allow creation of new VLANs up until there is 20 MB left of free memory (instead of 30 MB, which is what is happening currently).
PD4-3110253401	The command `show port rxerror` displays an error if the value for Rx jabber is too large {integer value too large to represent while executing "format "%8u" $xmlData(reply.message.show_ports_rxerrors.rxJabber)"}
PD4-2517224847	Maximum CPU sample limit on Summit series switches is limited to 1000 pps and this needs to be documented.
PD4-3330304159	In Summit X440 and X460 PoE capable switches, log message and SNMP traps are not generated when power usage threshold are reached.
PD4-3170880999	For Summit series switches, `show switch` command output shows incorrect information when switch is below minimum temperature.

Table 29: Resolved Issues, Platform-Specific and Feature Issues in ExtremeXOS 15.3 (Continued)

ID Number	Description
Summit X440 Series Switches	
PD4-3305963261	For Summit X440 series switches, bcm SDK for 5.9.4 is improperly indexing for setting registers on the qsgmii interface.
PD4-3178370231	Summit X440 switches are getting stuck at 29.5 C temperature and logging a hot spot temperature on the console instead of switch temperature when it reaches maximum limit.
PD4-3012552953	In Summit X440-8t series switches, 10/100/1000 Base-T link when speed is set to 100 Mbps with "AutoNeg Off", the link is coming up at speed of 1 Gbps and full-duplex mode in X440 and other end X460 link is coming up at speed 100 Gbps. Cannot ping between switches.
PD4-3013094551	In Summit X440-8t series switches, 10/100/1000 Base-T link when speed is set to 100 Mbps with "AutoNeg Off" between Summit x460 and x440. Observed BASET link is not coming up after restart ports. x460-48x x440-8t BASET 9 <------>9 10<-----> 10 Port (9, 10) in Summit X440-8t is not coming to active state after a save and reboot of the Summit x440 in the other DUT (Summit x460) ports (9, 10) link is coming up.
PD4-3311903079	CRC Error/bad packets should increment the RxError counter only, but the Congestion counter is incorrectly incremented as well.
Summit X450 Series Switches	
PD4-1673106807	For certain match conditions involving SIPv6 and DIPv6, packets may not hit an ACL in Summit X450a switches.
PD4-3253186902	Runtime diagnostics on Summit X450a switches fail with a XGM2-2Xf module with XFP installed.
Summit X460 Series Switches	
PD4-2700144775	Diffserv examination is not working at the GRE gateway at ingress from the LAN.
PD4-3092483478	QSFP+ direct-attach active optical cable does not link up when used with SummitStack-V80 stacking module in Summit X460 series switches.
PD4-3228083460	Links on VIM modules become active during bootup of switches before configuration is loaded. This occurs on Summit X460 series switches with XMG3-2sf and XMG3-4sf modules.
PD4-3212070797	On Summit X460 series switches, packets are not logged when icmp-type is used.
PD4-3187720889	Summit X460 series switches with XGM3SB-4sf modules show the wrong temperature value in the `show temperature` command output.
PD4-3092483593	The output for `show temperature` is not showing the correct maximum/normal temperature of the switch in stacking.

Table 29: Resolved Issues, Platform-Specific and Feature Issues in ExtremeXOS 15.3 (Continued)

ID Number	Description
Summit X480 Series Switches	
PD4-2839090271	IPv6 routes are missing in kernel after a port is restarted.
PD4-2839681491	When SX Mini-GBIC SFP is inserted after inserting and removing on that same port, the 100BASE-FX SFP, the link does not become active.
Summit X650 Series Switches	
PD4-2919055907	In Summit X650-24x series switches, 1000 BASE-BX-D/U, ZX and SX copper port fails to negotiate flow control capability with peer ports. As a result, flow control is always set to “none” after save and reboot.
Summit X670 Series Switches	
PD4-2940562102	DCBGP ends unexpectedly with signal-11 when adding/deleting 100 eBGP neighbors for a long duration.
PD4-3192082965	Traffic is not getting forwarded once the PFC Rx-pause is disabled. dot1p Traffic is sent from one device to another, and PFC receives accordingly. When the PFC Rx-pause is disabled at receiving device side, dot1p traffic is blocked in that port.
PD4-3185656278	Ethernet tx pause (802.3x) is not working across a slot in a stacking setup: (2 node stack - 160G stack) Slot-1 x670v-48t<--10G-->ixia-1 Slot-2 x670v-48x<--1G--->ixia-2 VIM: VIM4-40G4X sending traffic from ixia-1 to ixia-2 (rate-limit 2M) and expecting the Rx Ethernet pause at ixia-2 It looks like RX_PAUSE_EN is not getting enabled in 40G High Gig port.
PD4-3178905832	On Summit X670v switches with L2 LACP load sharing, traffic does not get forwarded on one of the member port after a save and reboot. Issue occurs with the following versions: ExtremeXOS 15.1.1.1, 5.1.2.12, and 15.2.1.
PD4-2823233670	oui and vpn-index range errors are printed in decimal.
PD4-2823233880	Add "(default)" to "both" keyword when configuring route-target.
PD4-3170880245	For Summit X670v-48t series switches, maximum local IPv4 hosts and IPv6 hosts are not allowed in the LPM and L3 hash table. Also, update theoretical maximum in legend of `show iproute reserved-entries statistics` command.
PD4-3116293491	QoS profile deletion is incorrectly allowed when the PFC rx-pause is enabled for the same QoS profile.
PD4-3116293726	Display shows both rx and tx are enabled when only one mode is enabled in PFC.
PD4-3185869422	Update temperature settings.
PD4-3334930168	In the *ExtremeXOS 15.X Concept Guide*, need to update the default stacking protocol for Summit X670 series switches.
E4G Cell Site Routers	
PD4-3346820155	Error "RMEP Creation Failed due to HAL problem" appears when creating 256 MEPs on E4G-200-12x cell site routers.

Table 29: Resolved Issues, Platform-Specific and Feature Issues in ExtremeXOS 15.3 (Continued)

ID Number	Description
PD4-2989427990	Log message appears "Unable to add route to unit 0, rc Entry exists. Shadow problem" during reboot.
PD4-2667034651	If a PTP clock port is configured as "slave-only", its state should show as "PTP- Slave" in "show network-clock ptp boundary port" output. However, "Master" appears, instead of "Slave-only".
PD4-2441010796	You can create more than 256 CES services on E4G cell site routers. After creating 496 CES services in E1 mode, there is no CES traffic between nodes in CES after 256 services. Only 256 CES services are working fine. Need to restrict number of services supported on the E4G cell site routers.
PD4-2983613821	For E4G-200 cell site routers, get error log message for added ring ports on control VLAN.
PD4-3253500300	Frequent warning level log messages appear for the timer expiration from CFM process.
PD4-3314862043	For E4G-400 cell site routers, you are able to assign non-existing QoS profile to CES Pseudowire.
AAA	
PD4-3404733231	AAA process ends unexpectedly when radius and tacacs servers are configured with a large input string as the shared-secret.
EAPS	
PD4-3086010511	ExtremeXOS 12.4.4-patch1-4: EAPS shared-port controller stuck in preforwarding [F] even with the shared port down. This can produce a super loop. Issue occurs when there are subsecond link flaps between the partner and controller.
PD4-3314858144	MLAG and EAPS: When an ISC port is part of multiple EAPS domains, and through the ISC port is not a secondary port on the master domain, and only a secondary port in transit domain, the MLAG peer configuration fails with an error.
PD4-3237904730	EAPS fail time range needs to be modified for milliseconds.
L3 VPN	
PD4-2778106871	VPN site temporarily loses route when secondary power is turned on or off.
MPLS	
PD4-3055296411	EXOS_LDP fails test 5.3 due to an internal log message warning for MPLS.
Optics	
PD4-3192802811	When 10G SFP+ passive copper cable is used, Rx errors occur on that port. This issue occurs on Summit X670v and BlackDiamond X8 series switches.
OSPF	
PD4-3101145181	OSPF external filter does not take effect until LSA ages out or it is forced by the refresh policy.
PD4-3423309981	With two adjacencies established, OSPFv3 process ends unexpectedly when link local address is replaced.

Table 29: Resolved Issues, Platform-Specific and Feature Issues in ExtremeXOS 15.3 (Continued)

ID Number	Description
Security	
PD4-3206070707	Deploying identity management (IDM) on ExtremeXOS 15.2 with Ridgeline 3.1 does not work properly. If IDM is deployed on earlier versions of ExtremeXOS, and then upgraded to ExtremeXOS 15.2, IDM functions properly.
PD4-3271740768	While using Dot1x and MAC-based netlogin on the same port, the MAC re-authentication timer should stop when the client is authenticated with dot1x credentials.
PD4-3157387244	Idmgr process ends unexpectedly after `configure identity-management delete ports all` command is issued.
PD4-3302318749	When solicited ARP violation is triggered on a LAG port, the following error message appears: <Erro:FDB.ArpError> Unable to retrieve pif, for slot:port=0:0.
PD4-3178933920	The command `unconfig identity-management` returns the error "no such variable" when no identity management configuration exists.
PD4-3238981482	Implement back door username and passwords, update patent numbers, and update copyright dates.
SNMP	
PD4-3417774715	In ExtremeXOS 15.X, several SNMP traps still appear as current in the newest MIB, even though they are using objects that are currently deprecated.
PD4-2770013137	SET operation on downloadControl table is not functioning.
PD4-2983106991	EXTREME-CFGMGMT-MIB:extremeLastSaveCfgTable has lexicographical error.
PD4-3033106992	Lexicographical error on extremeDownloadImageTable while walking for a stack setup.
PD4-3332155202	snmpMaster process ends unexpectedly with signal 6.
PD4-3333709136	When an SNMP get operation is performed from an SNMP manager and through CLI script, snmpMaster process ends unexpectedly with signal 6.
PD4-3174219240	snmpmaster memory leak occurs while polling from Ridgeline.
PD4-3146090044	SNMPv3 request authentication fails after switch reboot.
PD4-3240646472	SNMPv3 polling causes memory leak in snmpMaster process.
PD4-3291095414	snmpSubagent process ends unexpectedly while sending the snmpset with 1.3.6.1.2.1.3.1.1.1.2.1 OID.
PD4-3174250688	SNMP walk does not work after restarting snmpSubagent process.

Table 29: Resolved Issues, Platform-Specific and Feature Issues in ExtremeXOS 15.3 (Continued)

ID Number	Description
VLANs	
PD4-3269759161	Memory leak occurs after ending a telnet session with the `show vlan detail` command.
PD4-3158123625	In PVLAN configurations, when an IP address is configured for network VLANs, multicast traffic with a destination address 224.0.0.0/24 is sent back and forth between network VLANs. This affects switch's performance.
PD4-3316990558	Configuring translation VLAN as sub-VLAN causes mcmgr process to end unexpectedly.
PD4-3189051734	Need to update kernel error message when the switch receives the ARP-reply when there is no ARP entry for ARP-sender.

4 ExtremeXOS Documentation Corrections

This chapter lists corrections to the *ExtremeXOS 15.3 Concepts Guide* and *ExtremeXOS 15.3 Command Reference*.

This chapter contains the following sections:

ACLs

ExtremeXOS Concept Guide

Chapter 20: “ACLs”, under the heading “ACL Rule Syntax”

PD4-4367440234

The following text (bullet point):

“mirror—Sends a copy of the packet to the monitor (mirror) port (ingress only, and supported in egress only in x460 and E4G400 switches).”

Should be changed to:

“mirror—Sends a copy of the packet to the monitor (mirror) port (ingress only, and supported in egress only on Summit X460 series switches and E4G-400 cell site routers). Rules that contain mirror as an action modifier use a separate slice.”

ExtremeXOS Concepts Guide

Chapter 20: “ACLs”, under the heading “Apply ACL Policy Files”

PD4-4197196994

The following note should appear:

NOTE

If an ACL needs to be installed for traffic that is L3 routed and the ingress and egress ports are on different packet-processing units/ different slots with any of the following features enabled, then you should install the policy on a per-port basis, rather than applying it as a wildcard/ VLAN-based ACL:

- MLAG
- PVLAN
- Multiport-FDB

ExtremeXOS Concepts Guide

Chapter 20: “ACLs”, under the heading “Slice and Rule Use by Feature”

PD4-4152333000

The following note should appear:

NOTE

An additional rule is created for every active IPv6 interface and for routes with a prefix greater than 64 in the following modules for the BlackDiamond series switches. These rules occupy a different slice.

G48Ta,10G1xc,G48Te, G48Pe, G48Ta, G48Xa, 10G4Xa, 10G4Ca, G48Te2, G24Xc, G48Xc, G48Tc, 10G4Xc, 10G8Xc, S-G8Xc, S-10G1Xc

ExtremeXOS Concepts Guide

Chapter 3: “Managing the Switch”

xos0057249

The following text should be removed from multiple places under the indicated chapter:

- Only source-address match is supported.
- Access-lists that are associated with one or more applications cannot be directly deleted. They must be unconfigured from the application first, and then deleted from the CLI.
- Default counter support is added only for ACL rules and not for policy files. For policy files, you must configure count action.

Basic Switch Operation ExtremeXOS User Guide, Chapter 3: “Managing the Switch”

Policies and Security ExtremeXOS User Guide, Chapter 5: “ACLs” > “ACL Rule Syntax Details”

xos0058670

Change the match conditions fields "IGMP-type number" and "IGMP-code number" to "ICMP-type number" and "ICMP-code number".

The corresponding description fields state the correct match conditions (for example, "ICMP-type number" and "ICMP-code-number"), but the match condition fields are misprinted as "IGMP-type number" and "IGMP-code number", respectively.

BGP

ExtremeXOS Command Reference

command `enable bgp peer-group soft-in-reset`

PD4-2410195781

The following note is incorrect:

NOTE

If the specified peer group contains IPv6 peers, it is an IPv6 peer group and you must specify an IPv6 address-family. When the specified peer group is an IPv6 peer group, this command fails if no address family is specified or if an IPv4 address-family is specified. This command also fails if an IPv6 address family is specified for an IPv4 peer-group.

If you do not specify an address family, it defaults to IPv4 unicast. The command fails to execute, but this does not produce an error message.

ExtremeXOS Command Reference

command `enable bgp export`

PD4-4174873321

For the example, the text should change to:

“The following command enables BGP to export OSPF routes to other BGP routers: `enable bgp export ospf`”

Configure Access-List VLAN-ACL-Precedence Command Usage Guidelines

ExtremeXOS Command Reference for the `configure access-list vlan-acl-precedence` command

xos0060123

Change usage guidelines from:

"The following feature applies to only policy-file based ACLs that are applied on a VLAN. Use this command to switch between two VLAN-based ACL configuration modes. In the shared vlan-aclprecedence mode, VLAN-based ACL rules share the same precedence with other types of ACL rules. This is the default mode and provides the same behavior as in the previous software releases. In the dedicated vlan-acl-precedence mode, VLAN-based ACL rules have different precedence compared to other types of ACL rules. The dedicated mode yields improved installation performance for VLAN based access-lists but may affect hardware rule utilization in some configurations."

To:

"The following feature applies to only policy-file based ACLs that are applied on a VLAN. Use this command to switch between two VLAN-based ACL configuration modes. In the shared vlan-aclprecedence mode, VLAN-based ACL rules share the same precedence with other types of ACL rules and provides the same behavior as in the previous software releases. In the dedicated vlan-acl-precedence mode, VLAN-based ACL rules have different precedence compared to other types of ACL rules and this is the default mode. The dedicated mode yields improved installation performance for VLAN based access-lists but may affect hardware rule utilization in some configurations."

Configure IP-MTU VLAN Command Syntax Description

ExtremeXOS Command Reference and ExtremeXOS User Guide for the `configure ip-mtu` command

xos0061010

Command Reference

In the Syntax Description table, change the description from:

“mtu - Specifies the IP maximum transmission unit (MTU) value. Range is from 1500 to 9194.”

To:

“mtu - Specifies the IP maximum transmission unit (MTU) value. Range is from 1,500 to 9,194. However, the command allows the maximum limit up to 9,216 considering port configuration, such as tagging which influences the L2 header size. However, values greater than 9,194 may lead to packet loss and are not recommended.”

User Guide

Under the title *Jumbo Frames > IP Fragmentation with Jumbo Frames*:

Need to change the following content from:

“The ip-mtu value ranges between 1500 and 9194, with 1500 the default.”

To:

“The ip-mtu value ranges between 1,500 and 9,194, with 1,500 the default. However, the command allows the maximum limit up to 9,216 considering port configuration, such as tagging which influences the L2 header size. However, values greater than 9,194 may lead to packet loss and are not recommended.”

Debounce Commands

ExtremeXOS Command Reference

xos0060723

The following two debounce commands should appear:

Configure stack-ports debounce time

```
configure stack-ports {port-list} debounce time
[default|time]
```

Description

Configures debounce time feature on the stacking ports.

Syntax Description

port-list Specifies one or more stacking ports.

default Configure the default value “0”

<milliseconds> Time in milliseconds. Range is 0 (no debouncing) to 5000.

Default

Default debounce time value is 0

Usage Guidelines

Debounce timer can be configured to override the false link flaps i.e. link flaps that happens in a milliseconds interval.

Example

```
configure stack-ports 1:1 1:2 debounce time 150
```

History:

Available from ExtremeXOS 15.3.4

Platforms Availability

All stackable switches.

Show stack-ports debounce

```
show stack-ports {port-list} debounce
```

Description

Displays the current debounce time configured in stack-ports

Syntax Description

port-list Specifies one or more stacking ports.

Default

N/A

Usage Guidelines

To view the current debounce time configured in stack-ports. Specifying the stackport allows to view the debounce time for particular stack-port alone.

Example

show stack-ports 1:1 1:2 debounce

Following is the example output:

Stack Debounce

Port Time (ms)

----- --------------

1:1 0

1:2 0

History

Available from ExtremeXOS 15.3.4

Platform Availability

All stackable switches.

Denial of Service

ExtremeXOS Concepts Guide

Chapter 25: “Security” under the heading “Flood Rate Limitaton”

PD4-3957925332

The following note should appear:

NOTE

Summit X440, X460, X480, X650, X670 series switches; BlackDiamond 8900-MSM128 and BlackDiamond 8900-series I/O modules; and BlackDiamond X8-MM1 and series I/O modules, implement rate limiting granularity at millisecond intervals. The traffic bursts are monitored at millisecond intervals and actions performed within sub seconds (when applicable). When the switch evaluates the traffic pattern for bursts, against the configure value in pps, the value is calibrated per millisecond interval. For example: `configure port 1 rate-limit flood broadcast 1000` produces 1 packet per millisecond.

ELRP

ExtremeXOS User Guide

Section "Using ELRP to Perform Loop Tests”

xos0057320

The following known limitation of ELRP on VPLS service VLANs for Summit X480 series switches should appear:

“On Summit X480 series switches, ELRP does not detect a loop when enabled on a VPLS service VLAN. This is a hardware limitation.

You can work around this limitation using an ACL that copies the ELRP packets to the switch:

1 Find out the switch's MAC address and ELRP destination MAC address. The ELRP PDU's destination MAC address would be the switch MAC address with “01” for the first octet. For example, if the

switch MAC address is “00:04:96:51:12:32”, then the ELRP PDU's destination MAC address is “01:04:96:51:12:32”.

2 Create an ACL that moves the packets to the CPU that are destined to the ELRP destination MAC address and having Self MAC as the source address.

```
create access-list elrp_lift "ethernet-source-address
<switch_ethernet_source_address>; ethernet-destination-
address <ELRP_Dest>" "copy-cpu-and-drop"
```

In this example,

```
create access-list elrp_lift "ethernet-source-address
00:04:96:51:12:32; ethernet-destination-address
01:04:96:51:12:32" "copy-cpu-and-drop"
```

3 Now associate the access-list with the VPLS service VLAN on which the ELRP is to be enabled or apply it to the entire switch by the use of any option.

```
configure access-list add "elrp_lift" first any
```

or

```
configure access-list add "elrp_lift" first vlan
<vlan_name>
```

NOTE

While this procedure deals with this limitation, you use one more ACL rule. So, if there are other Extreme Network devices in the service VLAN network that do not run VPLS, then it is recommended that you enable ELRP on those devices instead of using this workaround which will consume ACL resources.

End of Support for BlackDiamond Platforms

ExtremeXOS Concepts Guide

Throughout the documentation

PD4-3291018828, PD4-4586509611

ExtremeXOS 15.2 does not support the following platforms. Any reference implying support is incorrect:

- BlackDiamond 10800 series switches
- BlackDiamond 12800 series switches
- BlackDiamond 20800 series switches

ICMP/IGMP

ExtremeXOS Concepts Guide

Chapter 25: “Security”

PD4-3282055971

The following information should appear in the ExtremeXOS Concepts Guide:

For the BlackDiamond X8 and Summit X670 series switches, it is not possible to have ICMP/IGMP code and type fields on egress. ICMP/IGMP type requires UDF (user defined fields). Ingress pipeline has UDF, but the egress pipeline hardware does not have UDF, so it cannot match ICMP/IGMP types on the egress pipeline.

IPMC-Hardware Flooding of Local-Network-Range (224.0.0.x)

ExtremeXOS Concepts Guide

Chapter 43: "Multicast Routing and Switching"

PD4-4214759988

The following information about the feature, IPMC-hardware flooding of local-network-range (224.0.0.x), should appear:

The IP multicast control packets (224.0.0.x) are slow-path flooded by default. Under scaled environment (lots of protocol instances and/or many ports in the VLAN) or due to high CPU utilization or congestion can produce packet losses.

When a VLAN is configured for L2 forwarding and *does not* have an IP address, entries are aged out periodically and re-learned. Periodic clearing of the IPMC FDB entry can result in:

- Temporary slow path forwarding
- Packet loss due to reprogramming of hardware entries

This feature enables the locally scoped address range (224.0.0.x) to get hardware (fast-path) flooded, and thus avoid packet losses. This is accomplished by a new additional rule installed in hardware. This feature does not consume a new ACL slice, rather it consists of a new rule. To switch the flooding mode from slow-path to fast-path and vice-versa, use the following command:

```
configure forwarding ipmc local-network-range [fast-path |
slow-path]
```

NOTE

Enabling this feature consumes one hardware ACL rule for each unit in per-port mode, and for each VLAN in per-VLAN mode. Check for availability of resources, such as ACL space and memory before enabling this feature. For optimal resource optimization when there are high numbers of VLANs, use per-port filters before enabling this feature.

The following platforms do not support this feature:

- Summit X350, X450e, X450 (original)
- BlackDiamond 8800 I/O modules G48Te, G48Pe, G48T, 10G4x, G24x, 10G4Xa, 10G4Ca.

Kerberos Snooping

ExtremeXOS Command Reference Guide

`configure identity-management kerberos snooping forwarding`

PD4-3689451863

The `configure identity-management kerberos snooping forwarding` command was added to ExtremeXOS 15.2, but was not included in the *ExtremeXOS Command Reference Guide*. The following information should appear:

Description

When identity management is enabled on a port, kerberos packets are software-forwarded. With this command, you can report if shared folder access via identity management-enabled ports is slow if there exists other CPU-bound traffic.

Syntax Description

forwarding	Configure how customer kerberos authentication packets are forwarded by this system.
fast-path	Forward customer snooped kerberos packets in hardware (default).
slow-path	Forward customer snooped kerberos packets in software. This option is recommended only for systems with low CPU-bound traffic.

Default

Fast-path.

Usage Guidelines

Use this command to report if shared folder access via identity management-enabled ports is slow if there exists other CPU-bound traffic.'

Example

```
The following show command displays the modified kerberos
information:
X460-48p.14 # sh identity-management
Identity Management : Enabled
Stale entry age out (effective) : 180 Seconds (180
Seconds)
Max memory size : 512 Kbytes
Enabled ports : 1
SNMP trap notification : Enabled
Access list source address type : MAC
Kerberos aging time (DD:HH:MM) : None
Kerberos force aging time (DD:HH:MM) : None
Kerberos snooping forwarding : Fast path
Kerberos snooping forwarding : Slow path
Valid Kerberos servers : none configured(all valid)
LDAP Configuration:
-------------------
LDAP Server : No LDAP Servers configured
Base-DN : None
Bind credential : anonymous
LDAP Configuration for Netlogin:
dot1x : Enabled
mac : Enabled
web-based : Enabled
```

History

```
This command was first available in ExtremeXOS 15.1.3.
```

Platform Availability

This command is available on all platforms.

Mirroring

Basic Switch Operation ExtremeXOS User Guide

Chapter 8: “Configuring Slots and Ports on a Switch” > “Mirroring” > “Guidelines for Mirroring”

xos0058665

The following text should appear:

Under “Summit Family Switches”:

“One-to-many remote mirroring does not work as expected where 'mirror-to' ports could receive double-tagged packets. This is due to hardware limitation and applies to the following platforms: Summit X150, X250e, X350, X450, X450e, and X450a”.

Under “BlackDiamond X8, BlackDiamond 8800 Series Switches and SummitStack”:

“One-to-many remote mirroring does not work as expected where 'mirror-to' ports could receive double-tagged packets. This is due to hardware limitation and applies to the following platforms: BlackDiamond G48T, G48P, 10G4X, G24X, a-series, e-series, c-series (except 8900 modules), and 8500 series modules.”

MLAG

ExtremeXOS User Guide, under *Basic Switch Operation* > *MLAG* > *MLAG-LACP*

xos0059921

Add the following note:

NOTE

When LACP shared ports are configured as MLAG ports, a LAG ID change after MLAG peer reboot may result in MLAG ports being removed and re-added to the aggregator. To avoid the MLAG port flap, it is recommended to configure a common LACP MAC in both the MLAG peers using the command `configure mlag peer <peer_name> lacp-mac <lacp_mac_address>`.

Multi-cast VLAN Registration

ExtremeXOS Concepts Guide

Chapter 42: “Multi-cast Routing and Switching” under the heading “Multi-cast VLAN Registration”

PD4-4356120873

The following note should appear:

NOTE

Multi-cast VLAN registration is not supported on Summit X430 series switches.

Network Login: Exclusions and Limitations

ExtremeXOS Concepts Guide

Chapter 23: “Network Login” under the heading “Exclusions and Limitations”

PD4-3833731450

The following note should appear:

NOTE

When STP with edge-safeguard and network login feature is enabled on the same port, the port goes into the disabled state after detecting a loop in the network.

Network Login: Web-Based Authentication

ExtremeXOS Concepts Guide

Chapter 23: “Network Login” under the heading “Web-Based Authentication”

PD4-4433918271

Under the heading “Configure the Redirect Page”, the following text:

‘By default, the redirect URL value is “http://www.extremenetworks.com”.’

Should be changed to:

‘By default, the redirect URL value is “http://www.extremenetworks.com” and default re-direction takes a maximum of 20 seconds (the default netlogin-lease-timer + 10 seconds). Re-direct time can be changed by tuning the netlogin-lease-timer.’

Policies and Securities

ExtremeXOS Concepts Guide

Chapter 20: “ACLs” > “Policy-Based Routing > Layer 2 Policy-Based Redirect

xos0057861

The following note should appear:

NOTE

"redirect-port" or "redirect-port-list" does not work for L3-switched packets matching ACL, if distributed IP ARP feature is turned on.

Policy Manager

ExtremeXOS Concepts Guide

Chapter 19: “Policy Manager” under the heading “Refresh Policies”

PD4-3929239241

The following note should appear:

NOTE

Refresh on multiple ports requires the original and modified policles to coexist at the same time in the intermittent state during refresh, and if this is not possible due to slice limitations, the refresh fails with a “ACL slice full“ error.

QoS

ExtremeXOS Concepts Guide

Chapter 20: “QoS and HQoS" under the heading “Displaying QoS Profile Traffic Statistics”

PD4-3593876589

The following note should appear:

NOTE

On a Summit X440 stack master slot, the QoS monitor displays the traffic packet count only for data traffic that is switched or routed. It does not capture the CPU/System-generated packet count.

RADIUS Server Client Configuration

ExtremeXOS Command Reference

Chapter 23: “Security Commands” under the `configure radius server client-ip` command

PD4-4385727966

The following note should appear::

NOTE

You should enable loopback mode on the VLAN associated with RADIUS if the RADIUS connectivity is established using a front panel port on a SummitStack.

Rate Limiting/Meters

ExtremeXOS User Guide for the configure ports qosprofile command

xos0057795

Need to include the following line above the example section:

"If max-burst-size has configured as "0", then it will use maximum available burst value."

Also, change the following:

“The max-burst-size parameter is the amount of traffic above the value in the cir-rate parameter that is allowed to burst from the port(s) for a short duration.”

To:

“The max-burst-size parameter is the amount of traffic above the value in the cir-rate parameter that is allowed to burst from the port(s) for a short duration. If max-burst-size has configured as "0", then it uses the maximum available burst value.”

Routing Policies

ExtremeXOS User Guide under Routing Policies > Routing Policy File Syntax > Policy Action Statements

xos0060766

In the Policy Actions table, for the "community set" attribute replace the existing text with the following text:

In the Action column:

“community set [no-advertise | no-export | noexport-76subconfed |

<community_num> | <as_num> : <community_num>];”

In the corresponding Description column:

“Replaces the existing community attribute of a route by the community specified by the action statement. Community must be enclosed in double quotes ("").”

Also, add the following note:

NOTE

Multiple communities cannot generally be used in “community set” attribute in a BGP policy file. However, you can effectively set multiple communities by using two sets of attributes as shown in following example:

```
entry permit-anything-else {

if {

} then {

community set "2342:6788";

community add "2342:6789 2342:6790";

permit;

}

}
```

Security

ExtremeXOS Concepts Guide

Chapter 25: “Security” under the heading “Authenticating Management Sessions Through a TACACS+ Server”

PD4-4155566039

The following note should appear:

NOTE

The switch allows local authentication when the client IP is excluded in the TACACS+ server by default. To disallow local authentication when the client IP is excluded in the TACACS+ server, use the local authentication disallow option.

sFlow Sampling

ExtremeXOS Concepts Guide and ExtremeXOS Command Reference

PD4-4347653204

ExtremeXOS Concepts Guide Change

Chapter 12: “Status Monitoring and Statistics” under the heading “Enable sFlow on the Desired Ports”

Under the first bullet point, the text:

“enable sflow ports port_list {ingress | egress | both}

The ingress, egress, and both options allow you to configure the sFlow type on a given set of ports. If you do not configure an sFlow type, by default ingress sFlow sampling is configured on the port.”

Should be:

“enable sflow ports all | port_list

By default ingress sFlow sampling is configured on the port.”

ExtremeXOS Command Reference Change

Chapter 13: “Commands for Status Monitoring and Statistics” under the command “enable sflow ports”

The command syntax:

“`enable sflow ports port_list {ingress}`”

Should be:

“`enable sflow ports all | port_list`”

Additionally:

- Remove the description of "ingress" from Syntax Description table.
- Under the heading “History”, remove the content "The ingress, egress, and both keywords were added in ExtremeXOS 15.3"

Show Ports Transceiver Information Command

ExtremeXOS Command Reference Guide

Chapter 6: “Commands for Configuring Slots and Ports on a Switch,” under the command `show ports transceiver information`

PD4-3928242896

The following note should appear:

NOTE

In the `show ports transceiver information` output, the Rx/Tx power values shown may be +/- 3dB from the actual value due to limitations of SFP and the accuracy depends on the SFP vendor. For accurate power measurement, it is recommended to use a power meter.

Software Upgrades

ExtremeXOS Concepts Guide

Appendix B: ”Software Upgrade and Boot Options” under the heading "Understanding Hitless Upgrade-Modular switches only"

PD4-3183278237

The following note should appear:

NOTE

Hitless upgrade is not supported on the BlackDiamond X8 series switches.

Synchronize Command

ExtremeXOS Command Reference for the `synchronize` command

xos0059976

The following text:

“ExtremeXOS software does not allow a synchronize operation on a SummitStack between a Summit X460 or X670 switch and a Summit X480 switch. If one is attempted, the following message is displayed:...”

Should be:

“ExtremeXOS software does not allow a synchronize operation on a SummitStack between a Summit X460 ,X670 or X440 switch and a Summit X480 switch. If one is attempted, the following message is displayed:...”

TACACS Server

ExtremeXOS User Guide under *Security > Authenticating Management Sessions Through a TACACS+ Server > Configuring the TACACS+ Client for Authentication and Authorization*

xos0060212

The following new topic should appear, Changing the TACACS+ Server:

To change a TACACS+ server configuration to avoid service interruption with respect to authentication and authorization:

NOTE

When only a single TACACS+ server is configured, you must disable TACACS-authorization (if enabled) before reconfiguring the TACACS+ server.

1. Unconfigure existing primary TACACS+ server (the TACACS+ server will failover to the secondary server) by issuing the following command:

   ```
   unconfigure tacacs server [primary | secondary]
   ```

2. Configure new primary TACACS+ server by issuing the following command:

   ```
   configure tacacs [primary | secondary] server [ipaddress
   |hostname] {tcp_port} client-ip ipaddress {vr vr_name}
   ```

3. Configure the shared-secret password for the primary TACACS+ server by issuing the following command:

```
configure tacacs [primary | secondary] shared-secret
{encrypted} string
```

NOTE

Only after configuring the shared-secret password for the primary server, TACACS+ will fallback to primary server from secondary.

4. Unconfigure the existing secondary TACACS+ server by issuing the following command:

   ```
   unconfigure tacacs server [primary | secondary]
   ```

5 Configure the new secondary TACACS+ server by issuing the following command:

```
configure tacacs [primary | secondary] server [ipaddress
| hostname] {tcp_port} client-ip ipaddress {vr vr_name}
```

6 Configure the shared-secret password for the secondary TACACS+ server by issuing the following command:

```
configure tacacs [primary | secondary] shared-secret
{encrypted} string
```

NOTE

The command `disable tacacs` is not required while changing TACACS+ servers, and it is recommended to “disable tacacsauthorization” (if enabled), before disabling TACACS+.

Unconfigure Switch Erase Command

ExtremeXOS Command Reference for the `unconfigure switch` command

xos0059832

Need to include the following information on the `unconfigure switch` command to explain `unconfigure switch erase`. Replace the content from the beginning of information on the command to the syntax description with the following content.

“unconfigure switch

```
unconfigure switch {all | erase [all | nvram]}
```

Description

Returns the switch configuration to its factory default settings and reboots the switch.

Syntax Description

`all` - Specifies that the entire configuration should be changed to the default values, including the management IP address, failsafe account, and SummitStack-specific parameters, and the switch is rebooted.

`erase all` – All data such as loaded ExtremeXOS images (both partition), configuration files, policy files, non-volatile memory content, and switch settings is overwritten. This renders the switch inoperable until you perform a bootrom rescue. The system reboots after the erase operation is complete, which takes around 10 minutes.

`erase nvram` - Data in non-volatile memory such as selected configuration, selection image partition, and log messages are overwritten. Switch boots up with primary image. Any unsaved configuration changes are lost and the switch reboots.”

Virtual Routers

ExtremeXOS Concepts Guide

Chapter 18: “Virtual Routers” under the heading “User Virtual Routers”

PD4-4042755165

The following note should appear:

NOTE

When using SNMPv2c for user-created virtual routers, set "Read community" in the SNMP tool to “vr_name@community_name”, where vr-name is the user-created virtual router name.

Similarly, for SNMPv3, set "Context name" in the SNMP tool to “vr_name@community_name”, where vr-name is the user-created virtual router name.

VLANs

ExtremeXOS Concepts Guide and *ExtremeXOS Command Reference*

Chapter 13: “VLANs”, under the heading “VLAN Configuration Overview”

PD4-4032146262

The command:

```
create vlan <vlan_name> {description <vlan-description>}
{vr <name>}
```

should be

```
create vlan <vlan_name> {tag name} {description <vlan-
description>} {vr <name>}
```

Also, in the *ExtremeXOS Command Reference*, add the description for *tag name* in the "Syntax Description" table: “tag name—Specifies a value to use as an 802.1Q tag. The valid range is from 2 to 4095.”

VRRP Guidelines

ExtremeXOS Concepts Guide

Chapter 31: “VRRP” under the heading "VRRP Guidelines"

xos0056279

The VRRP guidelines should change to the following:

“The following guidelines apply to using VRRP:

- The maximum number of supported VRIDs per interface is seven.
- An interconnect link between VRRP routers should not be used, except when VRRP routers have hosts directly attached.
- A maximum of 128 VRID instances are supported on the router. This number can be extended up to 256 based on the license and hardware; refer to the release notes for the maximum limit.
- Up to seven unique VRIDs can be configured on the router.
- VRRP and other L2 redundancy protocols can be simultaneously enabled on the same switch.
- We do not recommend simultaneously enabling VRRP and ESRP on the same switch.
- When VRRP and BOOTP/DHCP relay are both enabled on the switch, the relayed BOOTP agent IP address is the actual switch IP address, not the virtual IP address.
- VRRP and ESRP cannot be configured on the same VLAN or port.T his configuration is not allowed.
- RFC 5798 describes a situation where a master VRRP router takes on a duplicate IP address due to interaction with the duplicate address detection (DAD) feature. To prevent such duplicate addresses, the DAD feature is disabled whenever a VRRP router is configured for IPv6 or IPv4.
- A VRRP router instance can be configured with multiple IP addresses on the same subnet or on different subnets, provided that all virtual IP addresses match the subnet address of a VLAN on the switch. For example, if a host switch has VLAN IP addresses in the 1.1.1.x and 2.2.2.x subnets, then that VRRP router instance can contain virtual IP addresses in both those subnets as well.
- If a VRRP router instance is assigned priority 255, then the host router must own all the IP addresses assigned to the VRRP router instance. That is, each virtual IP address.”

VRRP Master Election

ExtremeXOS Concepts Guide

Chapter 30: “VRRP” under the heading "VRRP Master Election"

PD4-2820777108

The following note should appear:

NOTE

On BlackDiamond 8800 series switches, when a port belongs to two different VRRP instances with the same VRID, and one of the instances is a master VRID and the other a standby VRID, broadcast packets belonging to the standby VRRP VLAN generated by the master VRRP in that VLAN are not forwarded.

Window 95 References

ExtremeXOS Concepts Guide

Chapter 24: Network Login; Chapter 26: Security.

PD4-4625172859

All references to “Windows XP" should be replaced with "Windows 7/ Windows 8".